华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*）享有如下特权：

- **1、华为E-learning 课程学习**
  - **内容**：**所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式**：*关联证书*后，请提交您的“华为账号”和注册账号的“email”到 *Learning@huawei.com 申请权限。*
- **2、华为培训教材下载**
  - **内容：华为职业认证培训教材+华为产品技术培训教材**，覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入“*华为培训/面授培训*”，在具体课程页面即可下载教材。
- **3、华为在线公开课(LVC)优先参与**
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式**：开班计划及参与方式请详见*LVC排期*
- **4、学习工具 eNSP**
  - eNSP (Enterprise Network Simulation Platform)，是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外，华为建立了知识分享平台 华为认证论坛。您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。（http://support.huawei.com/ecommunity/bbs/list_2247.html）



HUAWEI构建内容安全网络

工程师培训上机指导书

（学员用书）

ISSUE 1.00



目录

1 手册说明

本手册用于指导学员学习华为安全产品的配置和部署技术，学员可以通过教材的实验说明，掌握本手册中的实验内容。

1.1 适用范围

适用于华为系统安全高级工程师培训安全课程中涉及的实验内容。

适用安全产品系列包括：

- USG2200/USG5100/USG5500
- NIP2000

特殊说明：USG2200/USG5100/USG5500 需要 V3R1 版本。

1.2 USG2200 产品描述

产品外观

USG2200 由一体化机箱、扩展接口卡组成。其一体化机箱尺寸为 442mm×414mm×43.6mm（宽×深×高），可以安装在 19 英寸标准机柜中。下面介绍 USG2200 的外观。

部件分布

USG2200 系列产品包含 USG2210、USG2220、USG2230、USG2250，都支持交流电源，其中 USG2250 还有支持直流电源的机型。

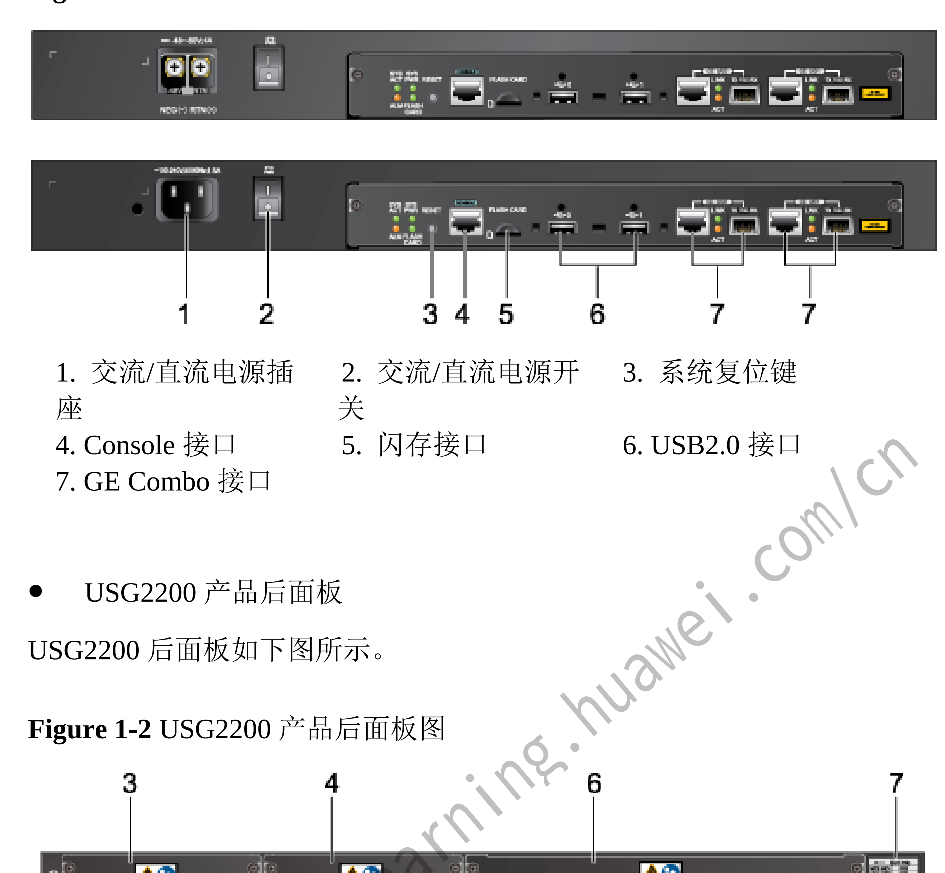
USG2210 分为普通配置和交流基本配置，普通配置为整机无扩展接口卡，交流基本配置为整机标配 2 个 5FSW 接口卡。

USG2220/2230/2250 分为普通配置和交流基本配置，普通配置为整机无扩展接口卡，交流基本配置为整机标配 2 个 1GE 接口卡。

- USG2200 产品前面板

USG2200 的前面板如下图所示。

Figure 1-1 USG2200 交流/直流机型前面板图

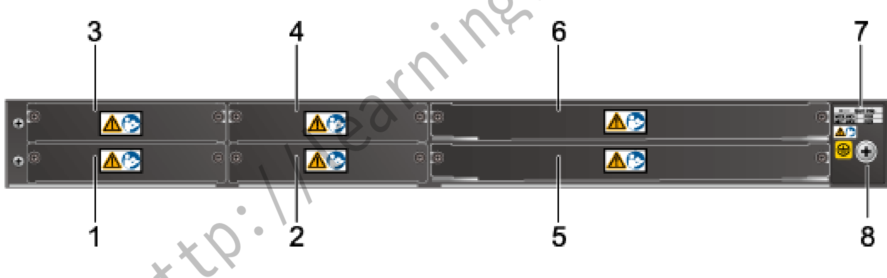


1. 交流/直流电源插座
2. 交流/直流电源开关
3. 系统复位键
4. Console 接口
5. 闪存接口
6. USB2.0 接口
7. GE Combo 接口

- USG2200 产品后面板

USG2200 后面板如下图所示。

Figure 1-2 USG2200 产品后面板图



1. MIC1/DMIC1 插槽
2. MIC2/DMIC2 插槽
3. MIC3 插槽
4. MIC4 插槽
5. FIC5/DFIC5 插槽
6. FIC6 插槽
7. 槽位标识
8. 接地端子

Figure 1-3 USG2210 基本配置型产品后面板图



Figure 1-4 USG2220/2230/2250 基本配置型产品后面板图



1.3 USG5120 产品描述

产品外观

USG5120 由一体化机箱、扩展接口卡组成。其一体化机箱尺寸为 442mm×414mm×86.1mm（宽×深×高），可以安装在 19 英寸标准机柜中。

部件分布

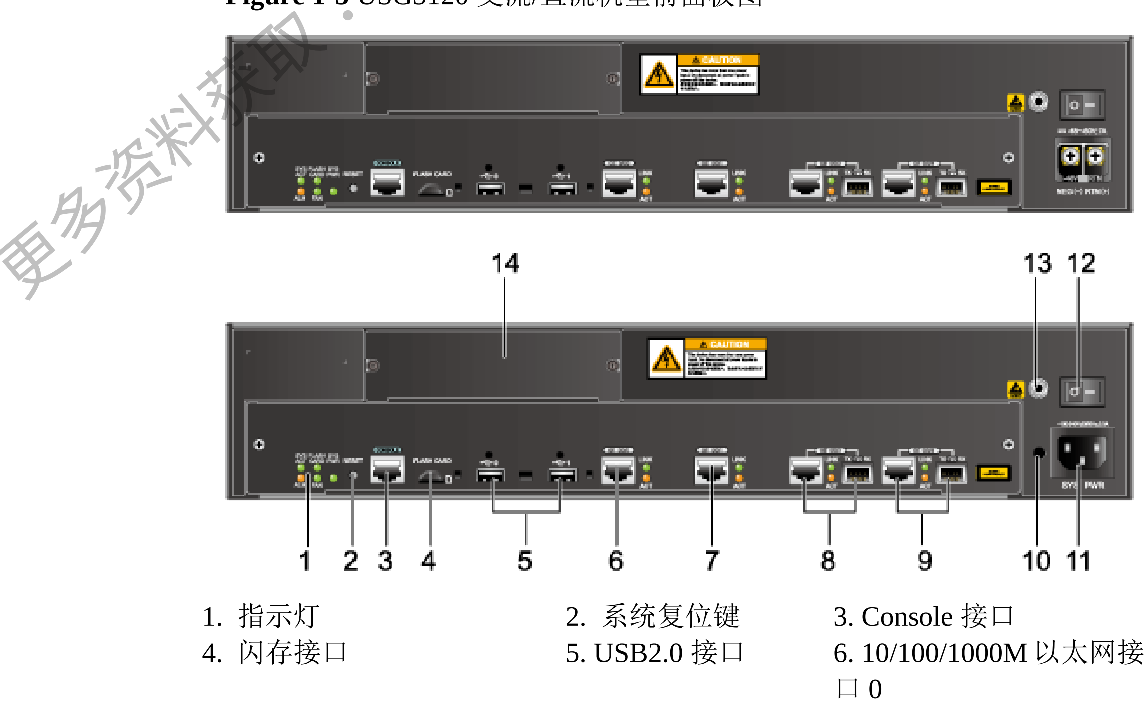
USG5100 系列产品包含 USG5120、USG5150 以及 USG5160。均由一体化机箱、扩展接口卡组成。

USG5120 有交流和直流两种机型。提供了 4 个 MIC 和 4 个 FIC 槽位，为 2U 高设备。USG5120 电源和风扇固定在设备中，不支持热插拔。

- USG5120 产品前面板

USG5120 的前面板如下图所示。

Figure 1-5 USG5120 交流/直流机型前面板图



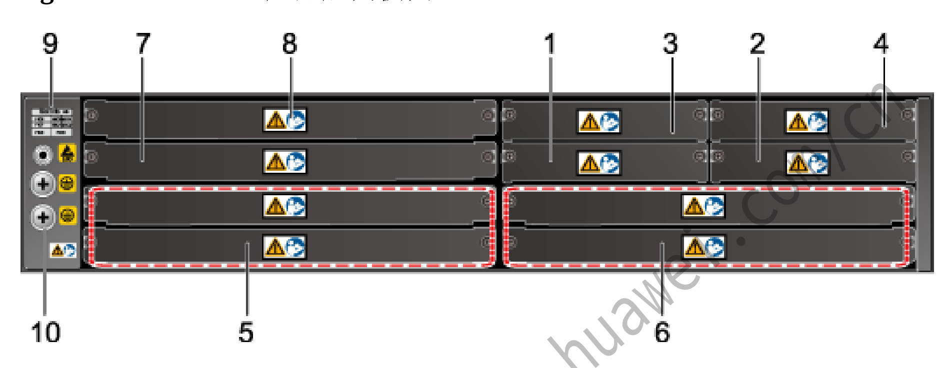
1. 指示灯
2. 系统复位键
3. Console 接口
4. 闪存接口
5. USB2.0 接口
6. 10/100/1000M 以太网接口 0

7. 10/100/1000M 以太网接口 1	8.GE Combo 接口 2	9.GE Combo 接口 3
10.卡扣插孔	11.交流/直流电源插座	12.交流/直流电源开关
13.防静电手腕带插孔	14.防尘面板	

- USG5120 产品后面板

USG5120 后面板如下图所示。

Figure 1-6 USG5120 产品后面板图



1. MIC1/DMIC1 插槽	2. MIC2/DMIC2 插槽	3．MIC3 插槽
4. MIC4 插槽	5. FIC5/DFIC5 插槽	6. FIC6/DFIC6 插槽
7. FIC7 插槽	8. FIC8 插槽	9. 槽位标识
10. 接地端子		

1.4 USG5150/USG5160 产品描述

产品外观

USG5150/USG5160 由一体化机箱、扩展接口卡组成。其一体化机箱尺寸为 442mm×414mm×130.5mm（宽×深×高），可以安装在 19 英寸标准机柜中。

部件分布

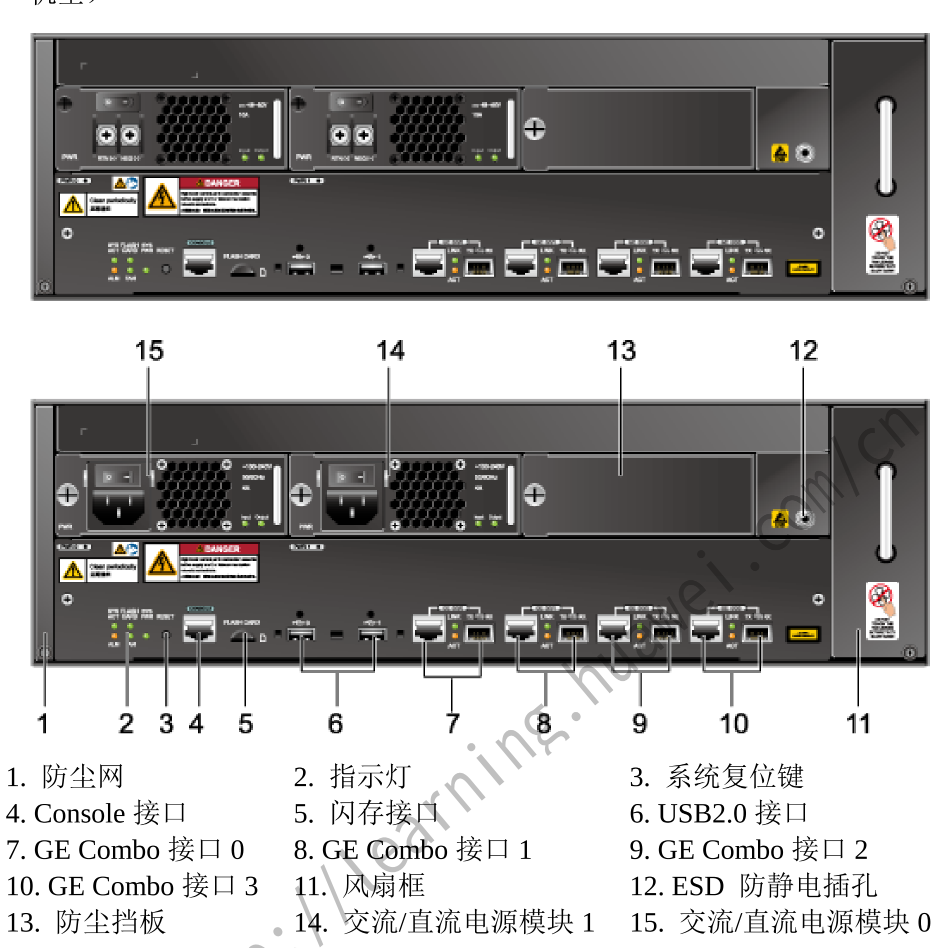
USG5150 电源可使用两个直流模块或两个交流模块，形成电源的负载分担。提供了 4 个 MIC 槽位和 6 个 FIC 槽位，为 3U 高设备。USG5150 的电源和风扇均支持热插拔。

USG5160 只有交流机型，可使用两个交流模块，形成电源的负载分担。提供了 4 个 MIC 槽位和 6 个 FIC 槽位，为 3U 高设备。USG5160 的电源和风扇均支持热插拔。

- USG5150/USG5160 产品前面板

USG5150/USG5160 的前面板如下图所示。

Figure 1-7 USG5150/USG5160 交流/直流机型前面板图（USG5160 无直流机型）

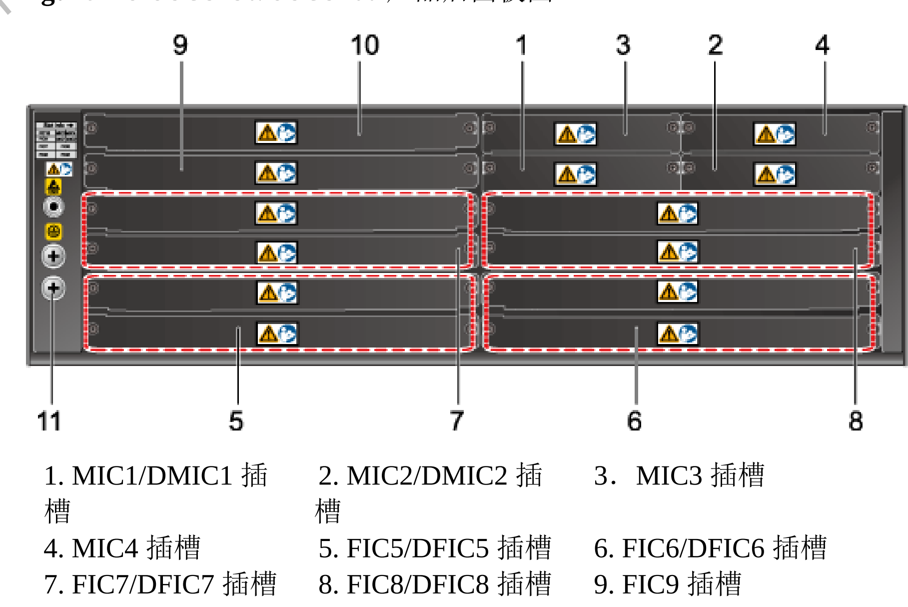


1. 防尘网 2. 指示灯 3. 系统复位键
4. Console 接口 5. 闪存接口 6. USB2.0 接口
7. GE Combo 接口 0 8. GE Combo 接口 1 9. GE Combo 接口 2
10. GE Combo 接口 3 11. 风扇框 12. ESD 防静电插孔
13. 防尘挡板 14. 交流/直流电源模块 1 15. 交流/直流电源模块 0

- USG5150/USG5160 产品后面板

USG5150/USG5160 后面板如下图所示。

Figure 1-8 USG5150/USG5160 产品后面板图



1. MIC1/DMIC1 插槽 2. MIC2/DMIC2 插槽 3. MIC3 插槽
4. MIC4 插槽 5. FIC5/DFIC5 插槽 6. FIC6/DFIC6 插槽
7. FIC7/DFIC7 插槽 8. FIC8/DFIC8 插槽 9. FIC9 插槽

10. FIC10 插槽　　11. 接地端子

插槽的排列顺序及接口编号方法

- 插槽排列顺序

USG 主板编号为 0，扩展插槽的槽位编号采用先从左到右，再从下到上，先MIC 槽位后 FIC 槽位的编号原则。

- 接口编号方法

设备接口采用的编号原则如下：

各接口按照从下到上，从左到右的顺序依次编号。物理接口编号为interface-type X/0/Y，interface-type 为接口类型（如 Ethernet 等），X 表示槽位号，0 为板卡号，目前支持的接口卡没有子卡，所以此位均为 0。Y 表示接口序号。主板的槽位号为 0。

1.5 NIP 产品描述

产品外观

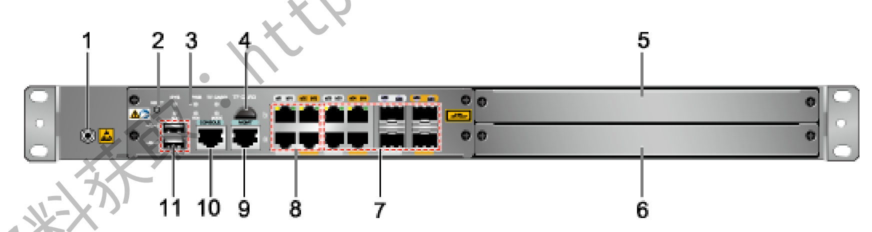
NIP2000 系列

介绍 NIP2000 系列的外观和基本参数。NIP2000 系列包括 NIP2100/2100D 和NIP2200/2200D。

部件分布

- NIP2100/2100D 前面板

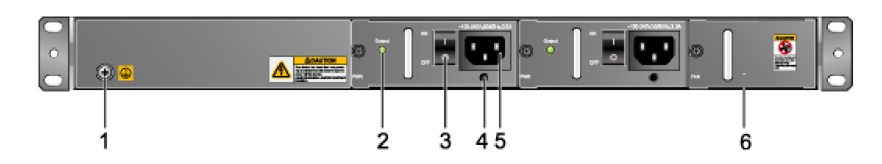
Figure 1-9 NIP2100/2100D 前面板



1. 防静电腕带插孔　2. 系统复位键　3. 指示灯区域
4. Micro-SD 卡插槽　5. FIC2 插槽　6. FIC1 插槽
7. 光电互斥接口　8. 10/100/1000M 自适应以太网电接口　9. 管理口
10. Console 接口　11. USB 2.0 接口

- NIP2100/2100D 后面板

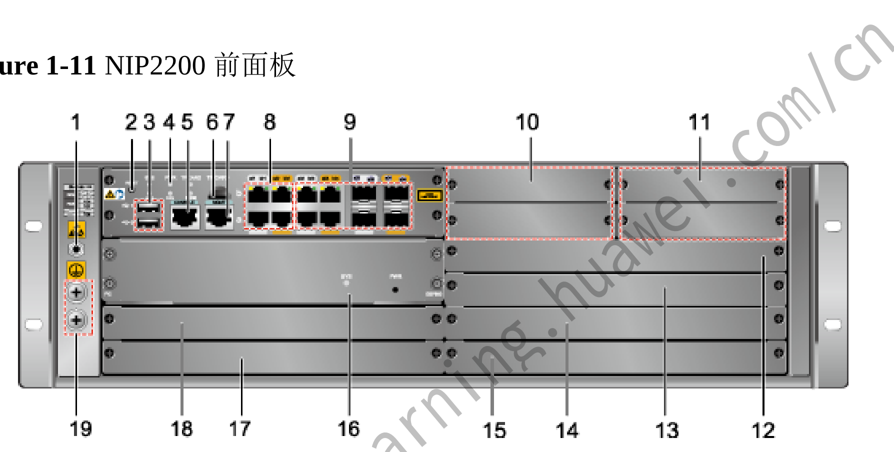
Figure 1-10 NIP2100/2100D 后面板



1. 接地端子　2. 电源指示灯　3. 电源开关
4. 交流电源线扎线孔　5. 电源接口　6. 风扇框

- NIP2200 前面板

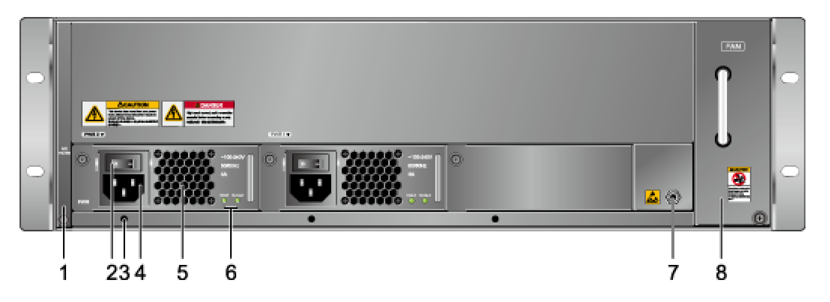
Figure 1-11 NIP2200 前面板



1. 防静电腕带插孔　2. 系统复位键　3. USB 2.0 接口
4. 指示灯区域　5. Console 接口　6. Micro-SD 卡插槽
7. 管理口　8. 10/100/1000M 自适应　9. 光电互斥接口
10. 假面板　11. 假面板　12. FIC9 插槽
13. FIC7 插槽　14. 假面板　15. FIC5 插槽
16. ESP800 卡　17. 假面板　18. 假面板
19. 接地端子

- NIP2200 后面板

Figure 1-12 NIP2200 后面板



1. 防尘网　2. 电源开关　3. 交流电源线扎线孔
4. 电源接口　5. 电源风扇网　6. 电源指示灯

7. 防静电腕带插孔 8. 风扇框

1.6 图示



2 NIP 基础实验

2.1 初始化配置 NIP 设备

实验目的

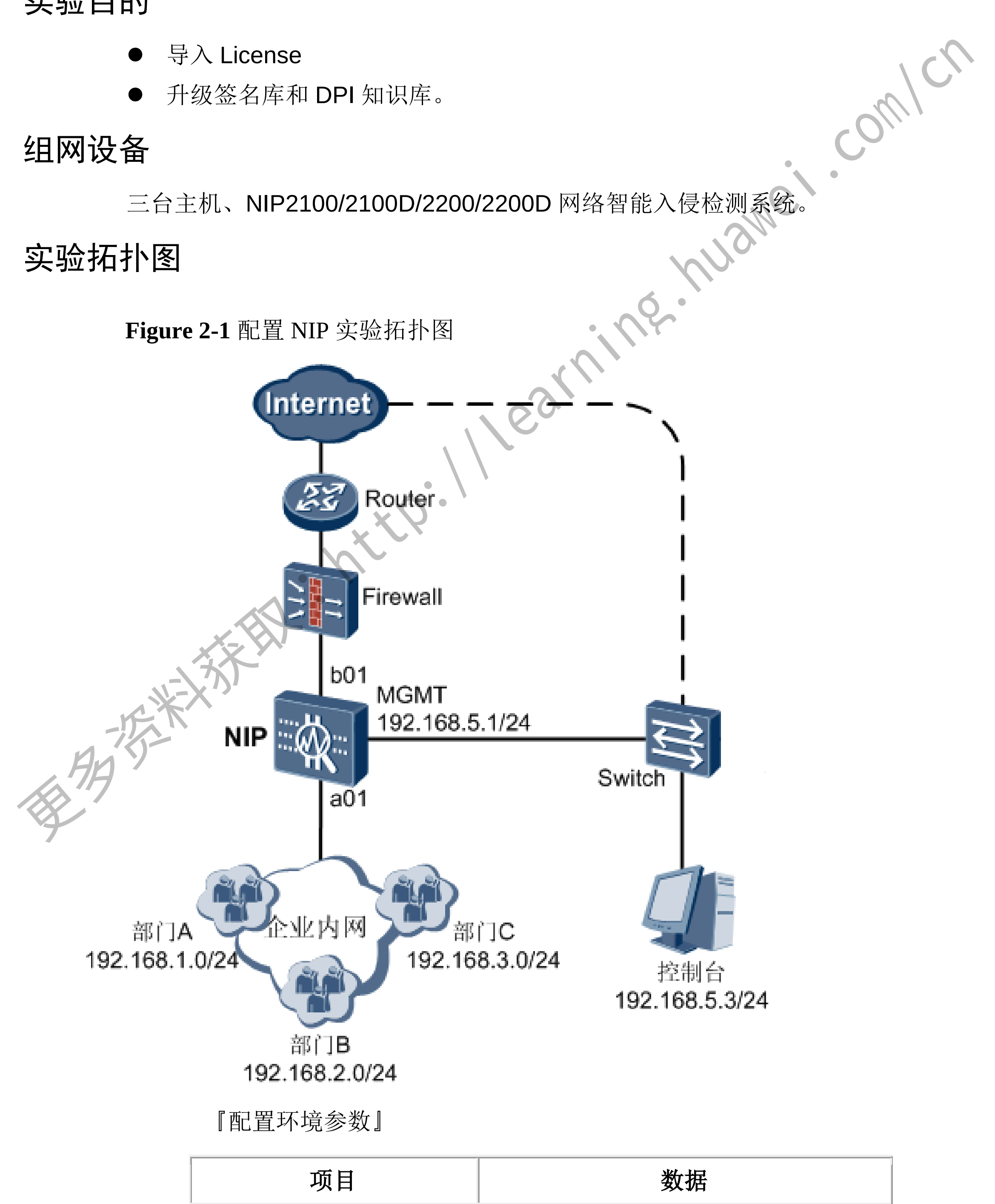
- 导入 License
- 升级签名库和 DPI 知识库。

组网设备

三台主机、NIP2100/2100D/2200/2200D 网络智能入侵检测系统。

实验拓扑图

Figure 2-1 配置 NIP 实验拓扑图



『配置环境参数』

项目	数据

项目		数据
NIP	接口：MGMT	IP 地址：192.168.5.1/24 默认网关：192.168.5.254 DNS 服务器：192.168.10.1
控制台		IP 地址：192.168.5.3/24 默认网关：192.168.5.254 DNS 服务器：192.168.10.1

配置步骤

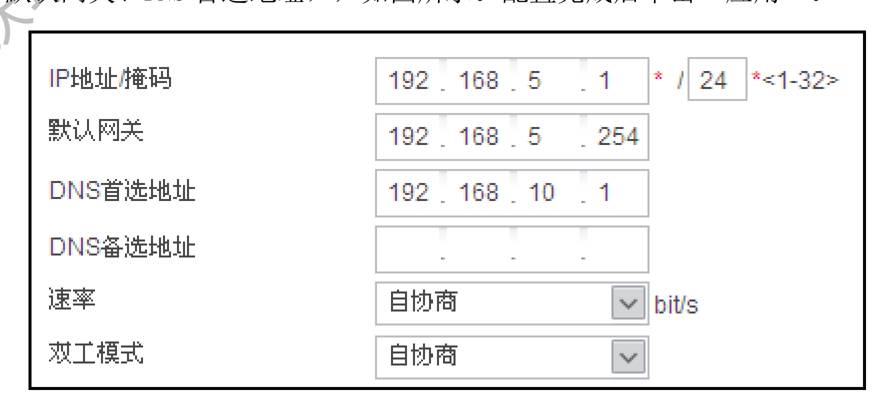
Step 1 配置 NIP 的基本参数。

以下步骤介绍的是通过 Web 界面配置 NIP 管理接口的 IP 地址/掩码、默认网关和 DNS 服务器，如果不能或者不方便登录 Web 界面配置，也可以通过 Console 口登录 NIP 的命令行来配置管理接口的 IP 地址/掩码和默认网关，然后再登录 Web 界面配置 DNS 服务器。

通过 Console 口登录 NIP 的命令行后，先执行命令 manage-ip 192.168.5.1 24 配置管理接口的 IP 地址/掩码，然后再执行命令 default-gateway 192.168.5.254 配置默认网关。

1) 将一台计算机（假设名称为 PC_1）的网口与 NIP 的管理接口直连或者通过二层交换机相连，将 PC_1 的 IP 地址配置为与 NIP 管理接口的 IP 地址在同一网段（例如 192.168.0.2/24）。在 PC_1 的浏览器中输入 http://192.168.0.1，然后输入用户名（admin）和密码（Admin@123）登录 NIP 的 Web 配置界面。登录后建议按照提示修改管理员密码，如果暂时不想修改请单击“取消”。

2) 选择“系统 > 配置 > 接口”，在接口状态图中单击接口 MGMT（状态图中标识为 MGMT/HA）的图标，按照数据规划配置管理接口的相关参数（IP 地址/掩码、默认网关、DNS 首选地址），如图所示。配置完成后单击“应用”。



3) 在控制台计算机的浏览器中输入 http://192.168.5.1，登录 NIP 的 Web 配置界面，单击界面右上角的“保存”，保存当前配置。

Note:修改完管理接口的基本参数、使用新的管理接口 IP 地址登录 NIP 的 Web 界面后，需要尽早保存当前配置，以免设备掉电重启后管理接口的基本参数恢复为缺省值。

Step 2 升级签名库和 DPI 知识库。

1) 激活 License。

- 选择“系统 > 维护 > License 管理”。
- 单击“上传”，在弹出的“上传文件”对话框中，单击“浏览”，选择 NIP 对应的 License 文件，单击“上传”。界面显示上传文件成功，则表示 License 文件已成功上传，列表中将添加新上传的 License 文件，此时状态为空。
- 单击 License 文件对应的，激活当前 License 文件。如果激活成功，则状态显示“当前 License 文件”，且该文件对应的 变为 。选择“监控 > 状态”后，“License 信息”中的“License 状态”应显示为“已激活”及其激活时间。

2) 配置定时升级签名库和 DPI 知识库。

由于 NIP 可以接入 Internet，所以此处以在线升级为例介绍，当 NIP 不能接入 Internet 时，请使用本地升级。

- 选择“系统 > 维护 > 升级中心”。
- 单击“修改”，依次配置各参数。
- “升级模式”选中“通过外网升级”。
- “安全服务中心域名”中输入需配置的安全服务中心的域名（本举例使用缺省值即可）。
- 选中“定时在线升级”，启用定时在线升级功能，并配置每日或每周定时在线升级的时间。
- 单击“应用”。

3) 选择“威胁防护升级”，单击“手动在线升级”，立即升级签名库；选择“应用控制升级”，单击“手动在线升级”，立即升级 DPI 知识库。

结果检查

选择“监控 > 状态”，“License 信息”中可以查看到签名库和 DPI 知识库的版本号。

2.2 直路部署 NIP

实验目的

直路部署 NIP

组网设备

三台主机、NIP1000\200\100 网络智能入侵检测系统

实验拓扑图

某企业有一条链路接入 Internet，内网所有计算机都可以访问 Internet，业务流量包含 Web 浏览、丰富的 P2P/IM 等用户上网业务。企业部署了 NIP 来保护客户端，防御针对客户端漏洞的威胁；同时防止内网计算机对网络的滥用。详细需求如下：

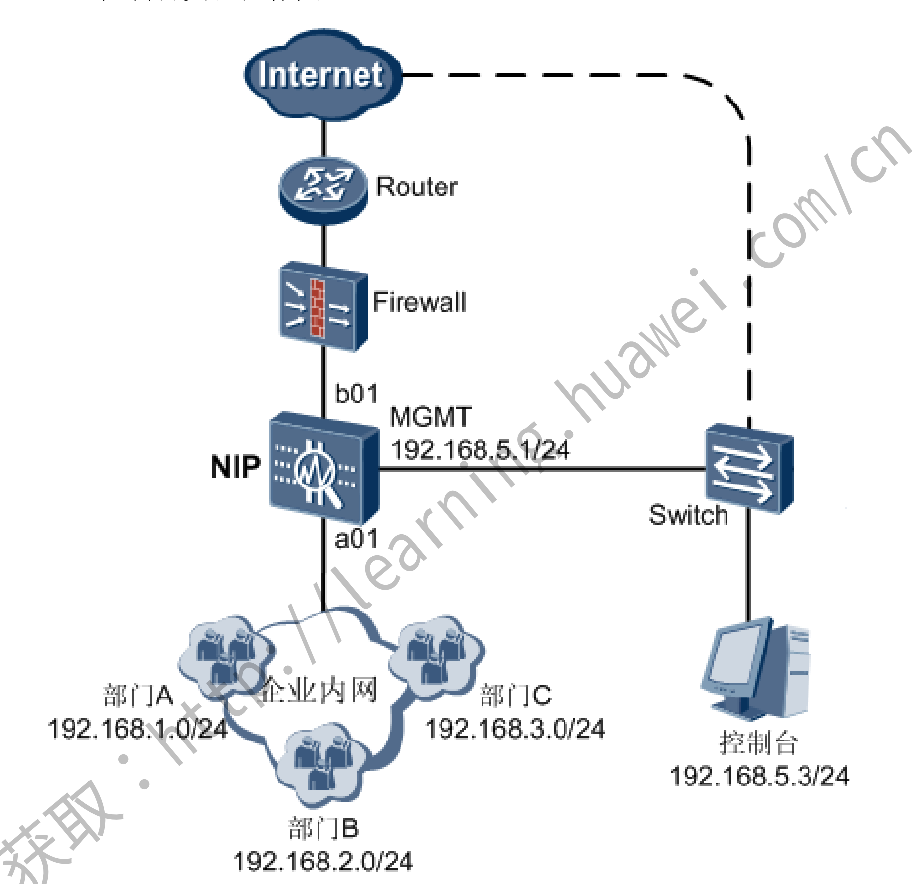
1） 防御来自 Internet 的针对客户端的威胁。

2） 每个部门的 P2P 流量速率都不超过 1Mbit/s。

3） 对 IM 软件（如 QQ、MSN 等）的使用限制如下：

- 部门 A 的客户端任何时间都不能使用。
- 部门 B 的客户端在工作时间不能使用。
- 部门 C 的客户端在任何时间都能使用。

Figure 2-2 NIP 控制台实验拓扑图



『配置环境参数』

项目		数据
NIP]	接口：MGMT	IP 地址：192.168.5.1/24 默认网关：192.168.5.254 DNS 服务器：192.168.10.1
	接口对：a01-b01	工作模式：IPS
	地址	名称：department_a 子网/IP 范围：192.168.1.0/24
	时间段	名称：work_time

项目		数据
		时间：每周一到周五的 09:00 到 12:00 和 13:00 到 17:00
	应用安全策略	**应用控制策略** 名称：policy_a、policy_b 和 policy_c 应用协议：P2P 和 IM 应用方向：a01->b01 **威胁防护策略** 名称：protect_client 策略模板：default_inline_ips 应用方向：a01->b01
控制台		IP 地址：192.168.5.3/24 默认网关：192.168.5.254 DNS 服务器：192.168.10.1

配置步骤

Step 1 配置 NIP 的基本参数。（略）

Step 2 配置公共对象，包括地址和时间段。

为了便于管理，将各部门的 IP 地址段定义为地址，访问的时间定义为时间段。

1） 配置地址。

a） 选择“公共对象 > 地址 > 地址”。

b） 单击“新建”，输入“名称”和“子网/IP 范围”，如所图 1 示。

图 1 新建地址“department_a”



c) 单击“应用”，完成地址的创建。

d) 按照同样的方法创建地址“department_b”和“department_c”。

2) 配置时间段。

a) 选择“公共对象 > 时间段 > 时间段”。

b) 单击“新建”，配置各参数，如图 5 所示。



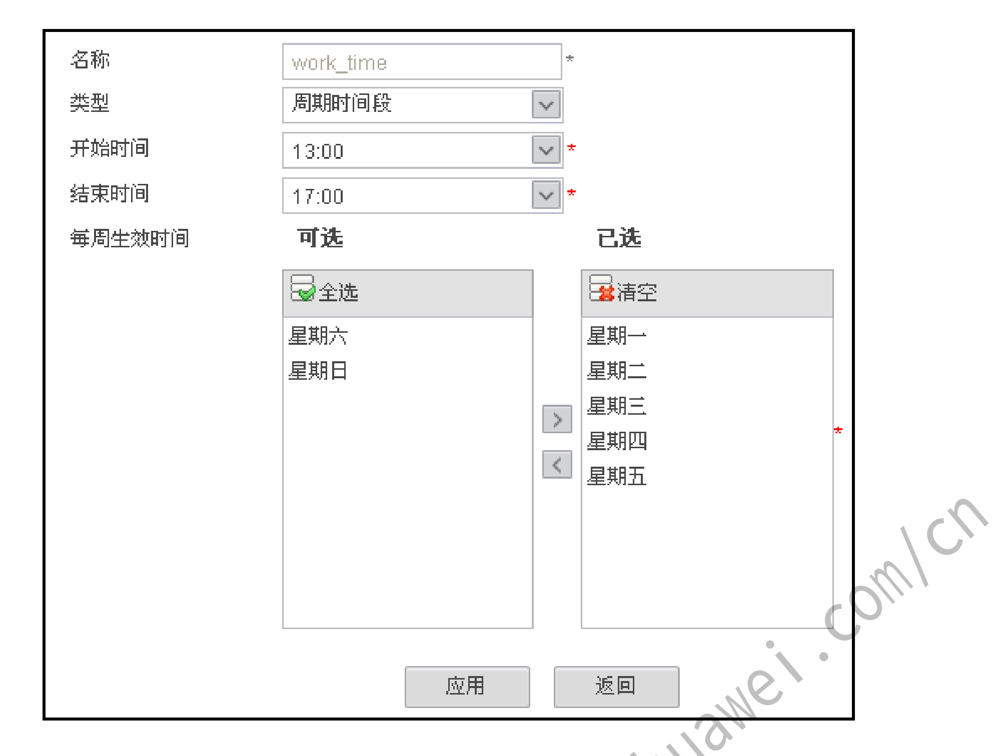
图 2 新建时间段“work_time”



c) 单击“应用”。

d) 单击时间段“work_time”对应的，增加成员，如图 3 所示。

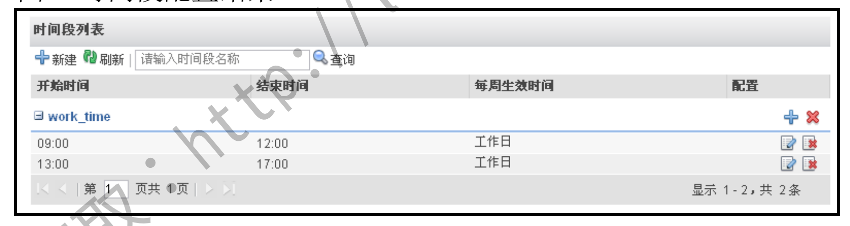
图 3 时间段“work_time”中增加成员



e) 单击“应用”，完成时间段的创建。

新创建的时间段“work_time”显示在“时间段列表”中，如图 4 所示。

图 4 时间段配置结果



Step 3 配置应用控制策略。

1) 选择“应用安全 > 应用控制 > 策略”。

2) 为部门 A 制定应用控制策略“policy_a”，P2P 流量不能超过 1Mbit/s，任何时间都不能使用 IM 软件。

a) 单击“新建”，输入策略的名称，如 5 所示。

图 5 新建应用控制策略“policy_a”



b) 单击“应用”，打开应用协议选择界面。

c) 单击“P2P”，“控制方式”中选择“限流及连接数限制”后，在“限流速率”中输入“1000”，如 6 所示。

图 6 配置 P2P 协议的控制策略



d) 单击“确定”。
e) 单击“IM”，使用缺省配置即可，如图 7 所示。

图 7 配置 IM 协议的控制策略

协议名称 IM
控制方式 阻断
时间段 all
确定 取消

f) 单击“确定”。
g) 单击“应用”，完成“policy_a”的创建。

3) 对部门 B 制定应用控制策略“policy_b”：工作时间不能使用 IM 软件，同时限制 P2P 的流量速率不能超过 1Mbit/s。

请参考“policy_a”的创建方式，不同之处为在配置 IM 时，“时间段”选择“work_time”。

4) 对部门 C 制定应用控制策略“policy_c”：对 IM 软件无限制，同时限制 P2P 的流量速率不能超过 1Mbit/s。

请参考“policy_a”的创建方式，不同之处为在配置 IM 时，“控制方式”选择“允许”。

新创建的应用控制策略“policy_a”、“policy_b”和“policy_c”显示在“应用控制策略列表”中，如图 8 所示。

图 8 应用控制策略配置结果


威胁防护策略列表

新建 刷新 导出 导入 提交

名称	引用	描述	状态	配置
default	是	Threat prevention policy	已提交	
protect_client	否	A policy that protects clients against threats	已提交	

Step 4 配置威胁防护策略。

1) 选择“应用安全 ＞ 威胁防护 ＞ 策略”。
2) 选择“配置全局参数”页签，配置威胁防护的全局参数，如图 12 所示，单击“应用”。图 12 中配置均为缺省配置，如果没有修改过，此项不需要配置。

图 9 配置威胁防护的全局参数



3) 新建策略“protect_client”。
   a) 选择“威胁防护策略”页签，在“威胁防护策略列表”中单击“新建”。
   b) 输入策略的“名称”和“描述”，并选择策略模板“default_inline_ips”，如图 10 所示。

图 10 新建威胁防护策略“protect_client”

名称	protect_client *
描述	A policy that protects clients against threats
同步策略/策略模板	default_inline_ips

c) 单击“应用”。

d) 单击“返回”，界面弹出是否立即提交的确认框，请单击“是”，等提交成功后单击“确定”。

新创建的威胁防护策略“protect_client”显示在“威胁防护策略列表”中，如图 11 所示。

图 11 威胁防护策略配置结果

威胁防护策略列表

新建 刷新 导出 导入 提交

名称	引用	描述	状态	配置
default	是	Threat prevention policy	已提交	
protect_client	否	A policy that protects clients against threats	已提交	

Step 5 将应用控制策略和威胁防护策略应用到 a01->b01 上。

1) 选择“应用安全 > 策略应用 > a01-b01”。

2) 单击“a01->b01”对应的，输入或选择“源地址”、“应用控制策略”和“威胁防护策略”，如图 12 所示。

图 12 将应用安全策略应用到 a01->b01



3) 单击“应用”。

4) 单击“a01->b01”对应的，应用部门 B 的策略。

部门 B 的策略与 A 类似，不同之处是源地址选 department_b，应用控制策略选 policy_b。

5) 单击“a01->b01”对应的，应用部门 C 的策略。

部门 C 的策略与 A 类似，不同之处是源地址选 department_c，应用控制策略选 policy_c。

配置完成后，可以看到相关部门已经和对应策略绑定，单击 移动策略的位置，如图 13 所示。

说明：

“ID”为 0 的策略是 NIP 缺省为接口对添加的策略。配置策略时，设备将根据配置的先后顺序从上往下排序策略，先配置的策略优先匹配流量。可以单击移动策略的位置，调整策略的优先级。

图 13 “a01->b01”绑定应用控制策略和威胁防护策略

ID	源地址	目的地址	服务	动作	应用控制策...	威胁防护策略	描述	命...	启用	配置
a01 → b01 (4 Items)										
1	department_a	any	ip	permit	policy_a	protect_client	--	0		
2	department_b	any	ip	permit	policy_b	protect_client	--	0		
3	department_c	any	ip	permit	policy_c	protect_client	--	0		
0	any	any	ip	permit	--	default	--	0		
b01 → a01 (1 Item)										
0	any	any	ip	permit	--	default	--	0		

Step 6 查看日志和报表。

1) 查看日志。

选择“监控 > 日志”，查看日志缓存区的日志信息。

2) 查看流量和威胁统计情况。

选择“监控 > 状态”，查看流量和威胁统计情况。

结果检查

客户端正常访问 Internet 的业务流量没有受影响。
每个部门的 P2P 流量速率都不超过 1Mbit/s。
各部门客户端使用 IM 软件已按照需求限制。
针对客户端的攻击流量已被 NIP 成功阻挡。

2.3 搭建攻击测试环境

实验目的

安装 SEAL 攻击软件。

组网设备

一台 Windos 32 位主机

实验拓扑图

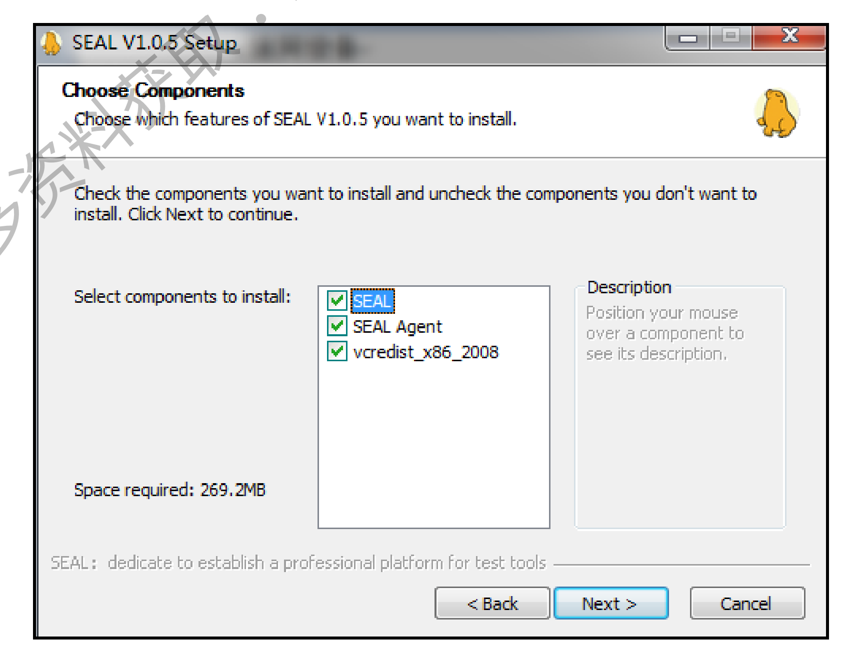
略

配置步骤

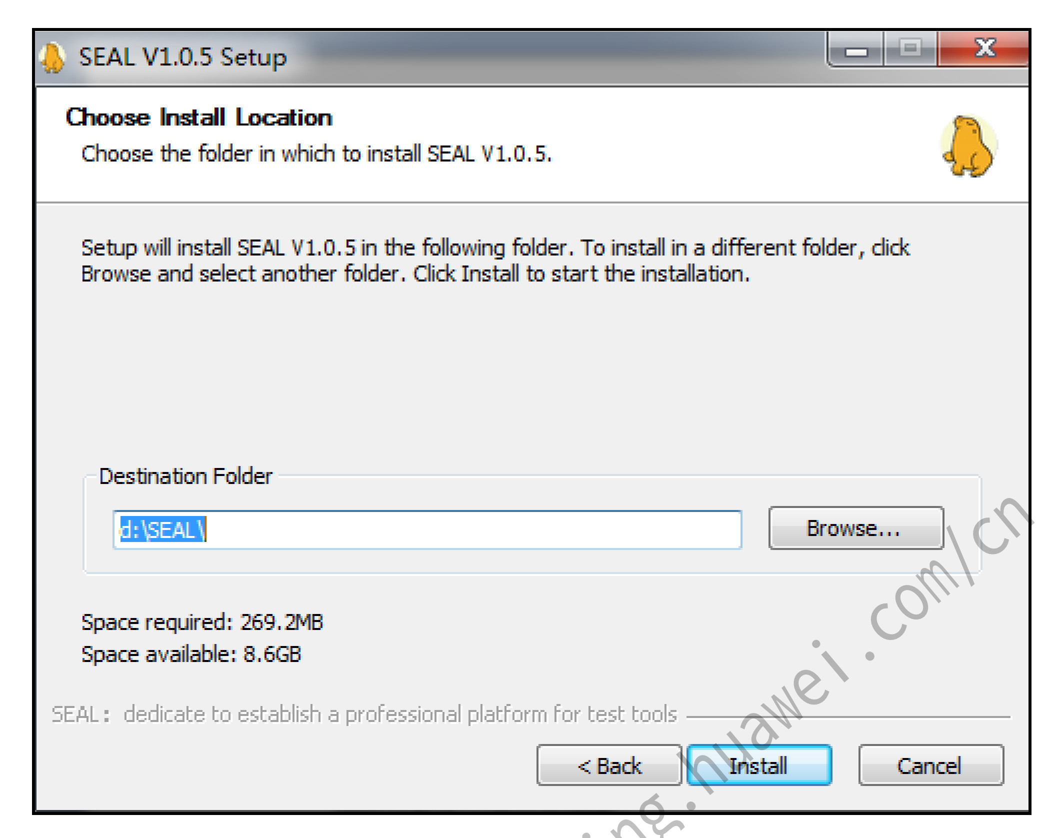
Step 1 双击 Seal 安装文件，开始安装 Seal。



Step 2 安装所有的 Seal 组件。



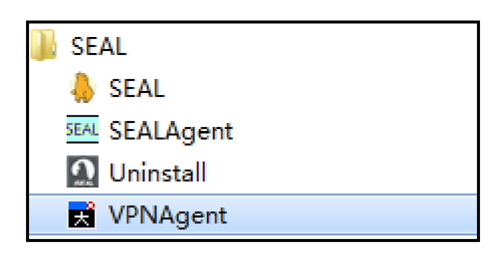
Step 3 指定安装目录，点击安装 Install 按钮。



Step 4 完成安装 Seal，并启动 Seal 程序。

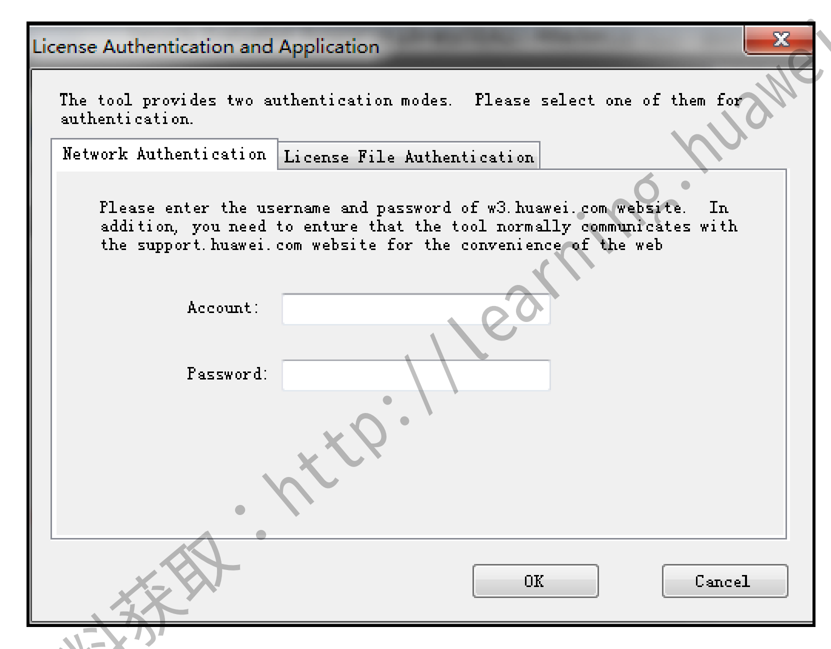


Step 5 启动 Seal 程序，首次启动。在开始所有程序中找到 Seal 程序目录，点击 SEALAgent，启动 Agent，然后在点击 Seal，启动 Seal 程序。



Step 6 启动 Seal 程序后，进入 license 认证页面。Seal 需要安装 License 才可使用。有俩种方法可以激活 License：

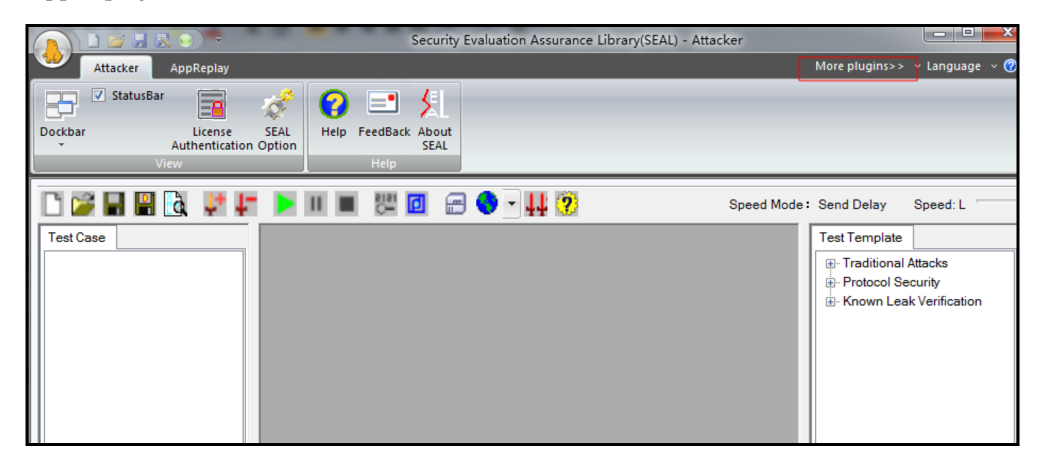
- 输入华为员工 W3 账号和密码，并点击 OK。此时保证 PC 连接华为公司内网，方可认证成功。
- 导入 License 文件，并点击 OK。此时方式需要收集本 PC 的 ESN，并填写至指定电子流中（http://3ms.huawei.com/hi/group/6349），可自动获取 License 文件。由于电子流在研发环境，必须委托研发同事代为在电子流中申请。



Step 7 完成 License 的操作后，添加相应的组件。

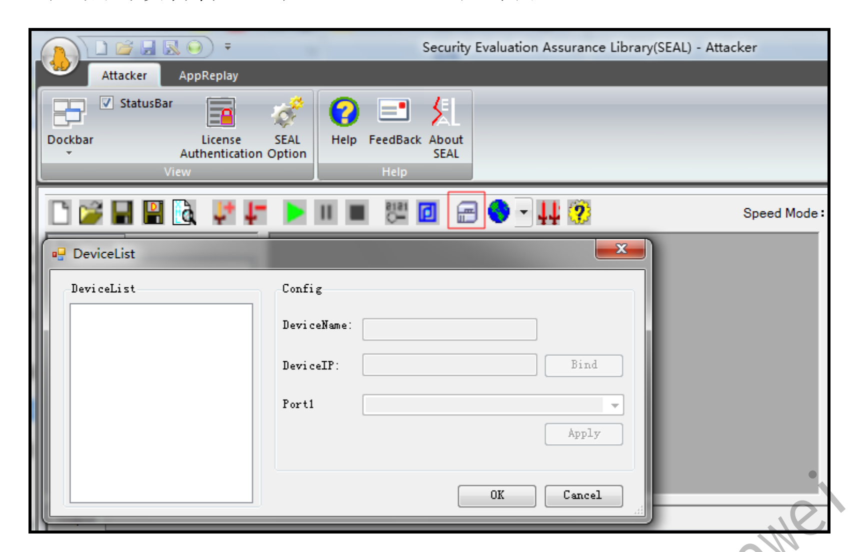
Attacker 用于模拟 DDos 攻击。

AppReplay 用于模拟入侵攻击。



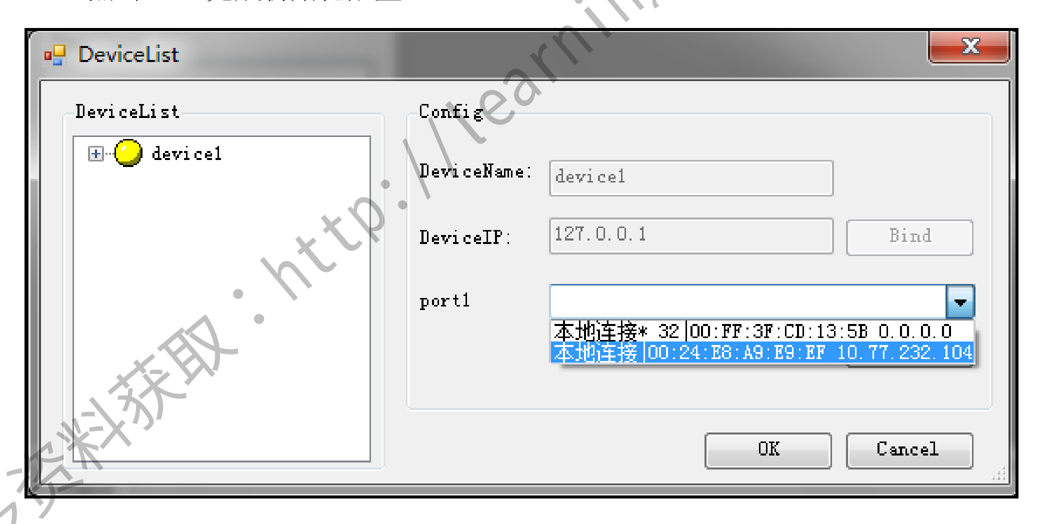
Step 8 配置 Attacker 页面，完成初始化配置。

1） 点击设备管理，在 Devicelist 处添加 Add Device



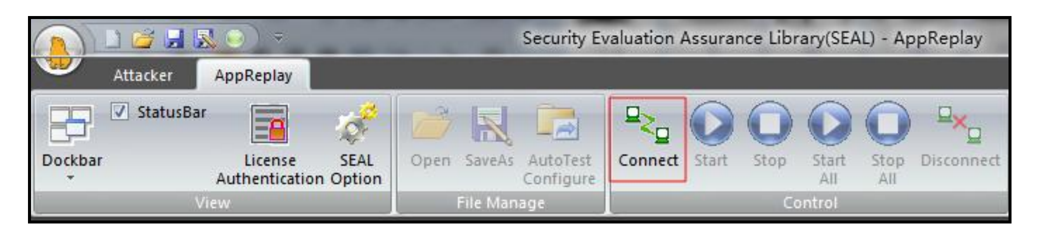
2） 输入主机 IP 地址为 127.0.0.1（固定本机环回地址），并点击 Bind。

3） 选择使用的网卡（可以通过 IP 地址判断具体的网卡），并选择 Apply，并点击 OK。完成初始化配置。

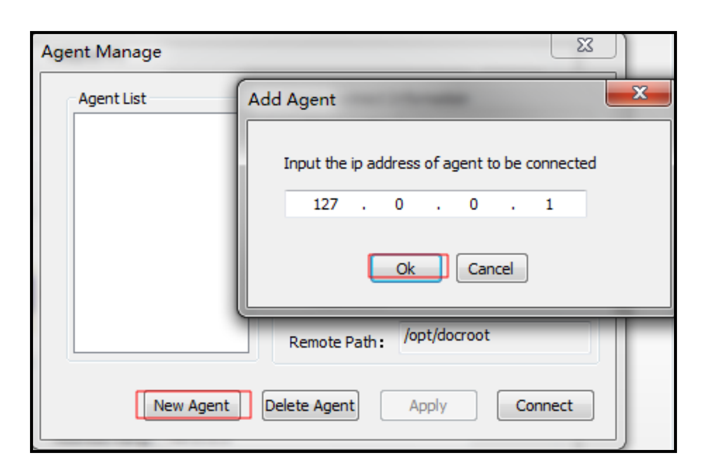


Step 9 配置 AppReplay 页面，完成初始化配置。

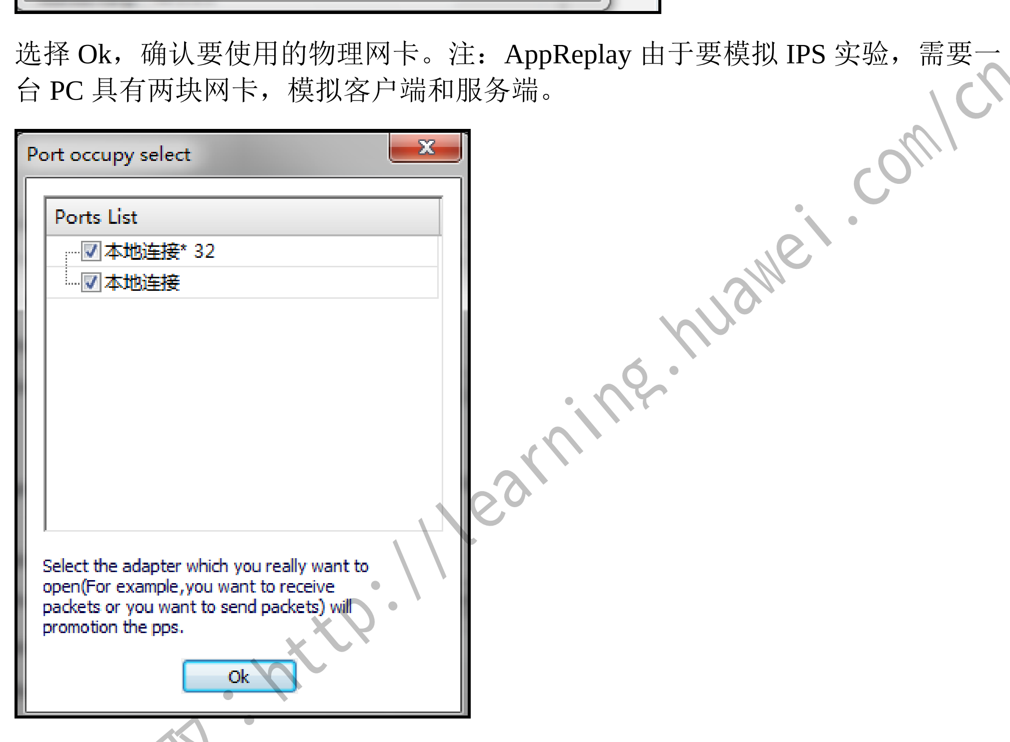
1） 点击 AppReplay，并点击 Connect。



2） 选择 New Agent，添加新的 Agent，并填入 127.0.0.1 IP 地址，然后点击 ok 按钮，保证连接到具体的物理网卡。最后点击 Apply，Connect 按钮，连接到具体的网卡。



选择 Ok，确认要使用的物理网卡。注：AppReplay 由于要模拟 IPS 实验，需要一台 PC 具有两块网卡，模拟客户端和服务端。



结果检查

无

3 UTM IPS 实验

3.1 IPS 基础配置实验

实验目的

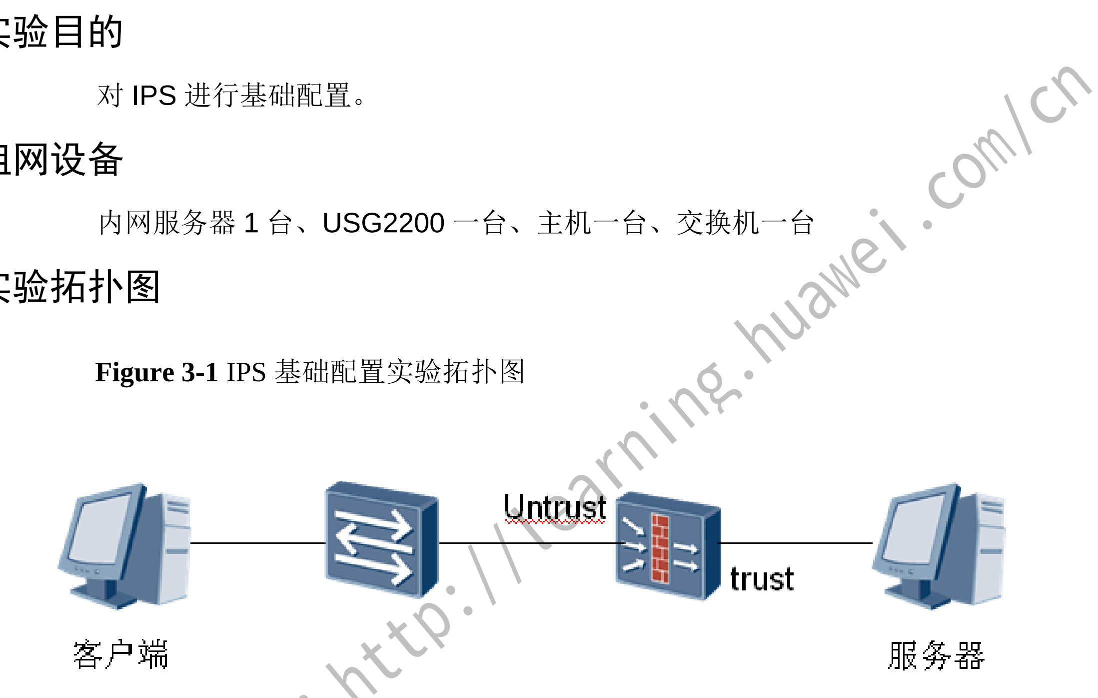
对 IPS 进行基础配置。

组网设备

内网服务器 1 台、USG2200 一台、主机一台、交换机一台

实验拓扑图

Figure 3-1 IPS 基础配置实验拓扑图



配置步骤

Step 1 对 USG5300 进行初始化配置

```
<USG> system-view
[USG] interface Ethernet 0/0/0
[USG-Ethernet0/0/0] description   **Connect_to_Switch****,
[USG-Ethernet0/0/0] ip address 192.168.1.1 24
[USG-Ethernet0/0/0] quit
[USG] interface Ethernet 0/0/1
[USG-Ethernet0/0/1] description   **** connect_to_Servers****,
[USG-Ethernet0/0/1] ip address 10.10.1.1 24
[USG-Ethernet0/0/1] quit
```

Step 2 获取 UTM License 许可

系统 > 维护 > License管理

License管理

License激活方式　◉ 在线自动激活　○ 本地手动激活

License中心域名　lic.huawei.com *

License授权编码　*

激活

License资源	状态
虚拟防火墙	已授权（100个虚拟防火墙）
SSL_VPN	已授权（100个并发用户）

系统 > 维护 > License管理

License管理

License激活方式　○ 在线自动激活　◉ 本地手动激活

文件　浏览...

激活

License资源	状态	
虚拟防火墙	已授权（100个虚拟防火墙）	
SSL_VPN	已授权（100个并发用户）	
入侵防御	已授权（过期时间：2012/10/13）	
版本号：	20110915.011	[升级配置]

License资源	状态	
虚拟防火墙	已授权（100个虚拟防火墙）	
SSL_VPN	已授权（100个并发用户）	
入侵防御	已授权（过期时间：2012/10/13）	
版本号：	20110915.011	[升级配置]
签名库版本：	20110915.011（升级时间：09:35:22 2012/09/12）	
反病毒	已授权（过期时间：2012/10/13）	
版本号：	20111017.003	[升级配置]
签名库版本：	20111017.003（升级时间：10:26:30 2012/09/12）	
垃圾邮件过滤	已授权（过期时间：2012/10/13）	
URL预定义分类查询	已授权（过期时间：2012/10/13）	[激活]

Step 3 升级 UTM 特征库



注：激活码会自动生成，在保证 License 文件导入的前提先，并保证设备已经连接到 Inetenet 上，点击激活，激活在线升级功能。

入侵防御

版本号	20110915.011
引擎版本	4.5.6.37
引擎大小	5757574 bytes
签名库版本:	20110915.011
签名库大小	471946 bytes
升级时间	09:35:22 2012/09/12
升级文件发布时间	21:26:02 2011/09/15

版本回退　出厂版本

升级

在线升级

☑ 定时在线升级

◉ 每日　01 : 03 *

○ 每周

手动在线升级

本地升级

文件　选择

本地升级

应用控制

知识库版本:	2.0.0.155
引擎版本:	DPI-Engine V100R002C02SPC300
加载时间:	2013/11/14 09:54:51
发布时间:	2012/09/07 06:32:48

版本回退

在线升级

升级后保存新的知识库文件 ☑ 启用

自动升级周期 90 <1-365>天

手动在线升级

本地升级

文件　选择

本地升级

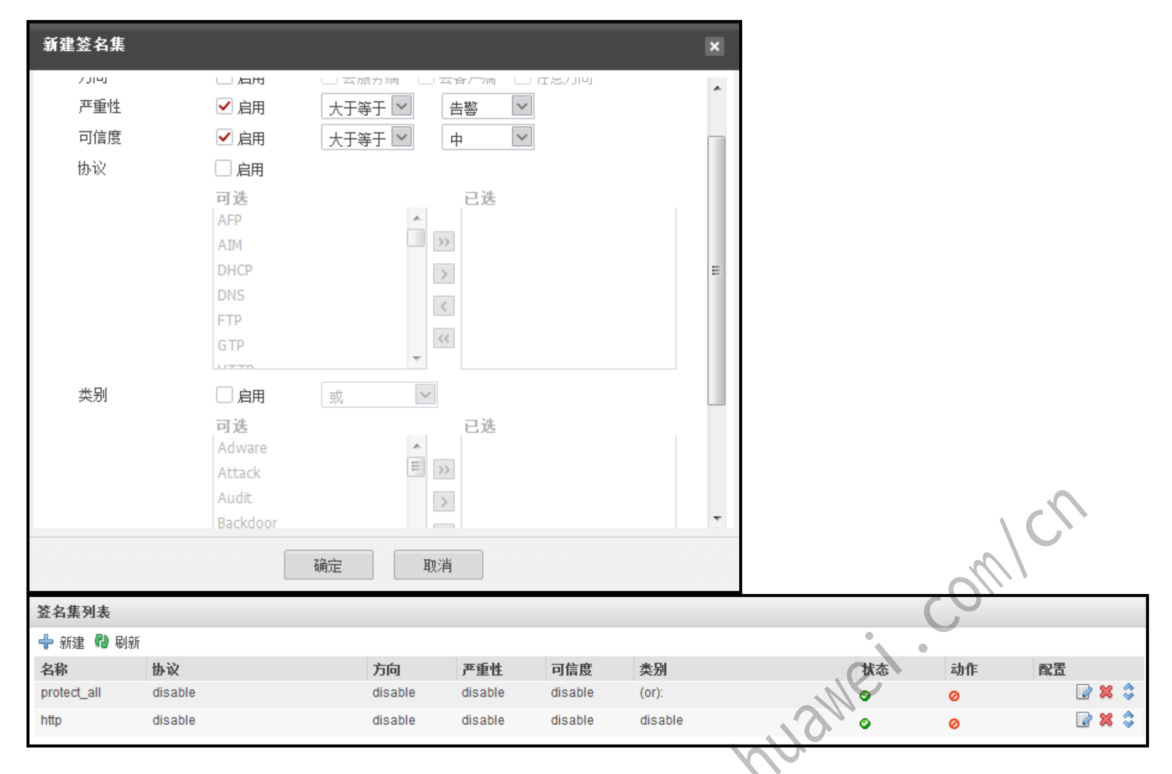
Step 4 设置防火墙工作在 UTM 模式



Step 5 使能 IPS 功能



Step 6 配置 IPS 签名集



Step 7 配置 IPS 转发策略



结果检查

访问 UTM 配置界面检查 IPS 配置

3.2 IPS 阻断攻击实验

实验目的

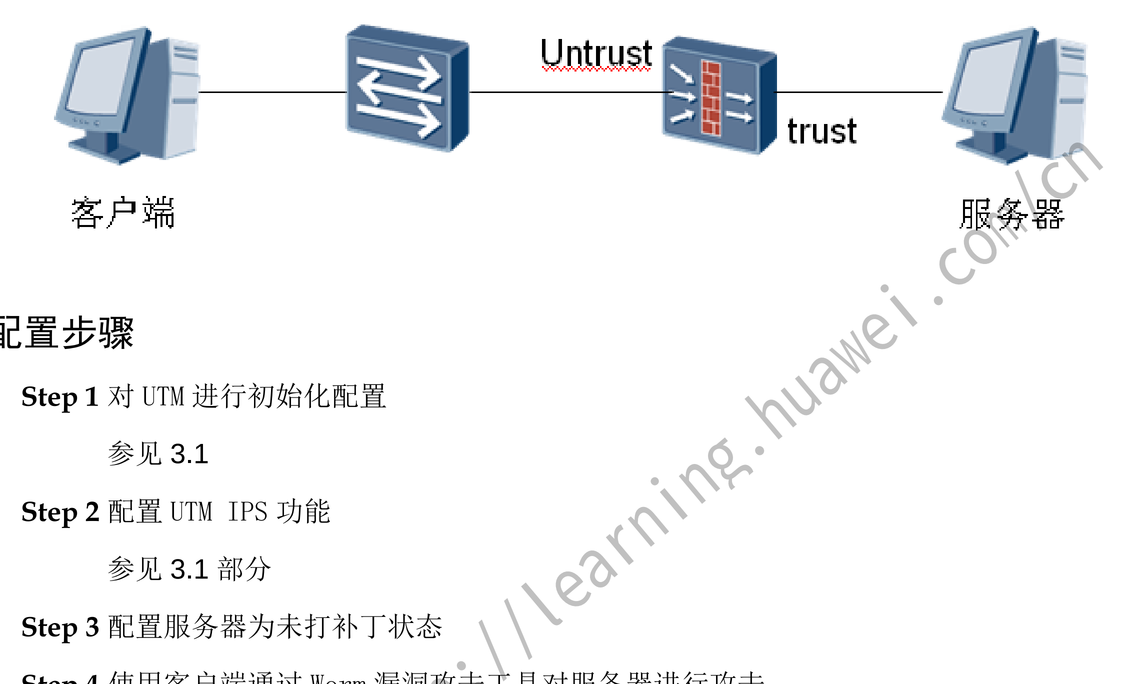
实现通过配置 IPS 实时阻断攻击。

组网设备

USG2200 一台、主机两台、交换机一台

实验拓扑图

Figure 3-2 IPS 阻断攻击实验拓扑图



配置步骤

Step 1 对 UTM 进行初始化配置

参见 3.1

Step 2 配置 UTM IPS 功能

参见 3.1 部分

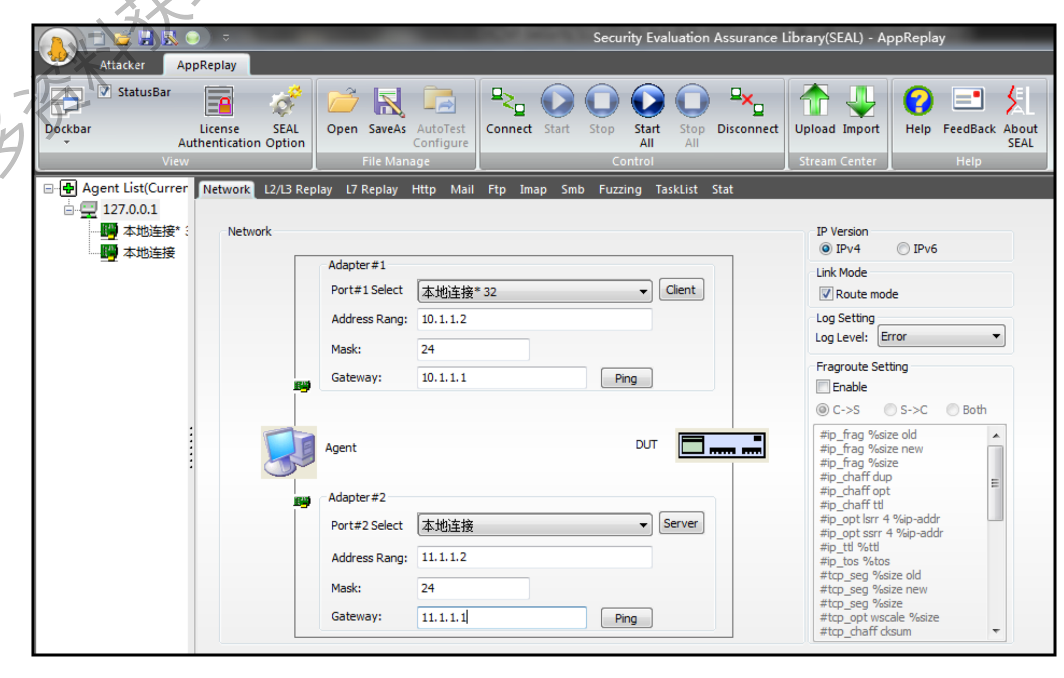
Step 3 配置服务器为未打补丁状态

Step 4 使用客户端通过 Worm 漏洞攻击工具对服务器进行攻击

1) 启动 Sear 的 AppReplay 组件。

Link Mode 选择 Route Mode，Route Mode 需要设置网关。

并在设置两个网卡的 IP 地址和网关。



2) 选择 L2/L3replay 点击 Add 按钮，点击 File Browser，添加攻击模拟包。并点击开始 

按钮。

结果检查

先关闭 USG2200 的 IPS 功能，测试客户端主机对服务器主机的攻击能否完成。

打开 USG2200 的 IPS 功能，测试能否阻断客户端主机对服务器主机的攻击。

4 UTM 防病毒实验

4.1 应用服务器防病毒攻击实验

实验目的

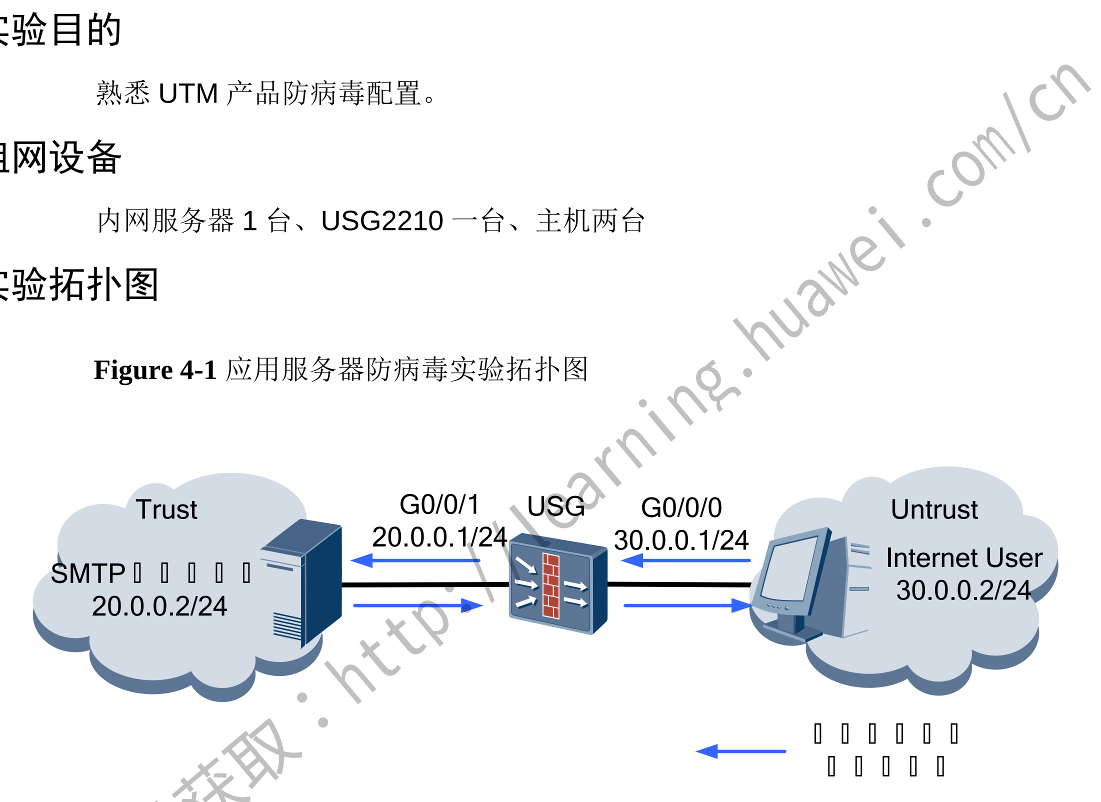
熟悉 UTM 产品防病毒配置。

组网设备

内网服务器 1 台、USG2210 一台、主机两台

实验拓扑图

Figure 4-1 应用服务器防病毒实验拓扑图



企业内部用户位于 Trust 区域，应用服务器（SMTP 邮件服务器）位于 DMZ 区域，Internet 上的用户位于 Untrust 区域，企业内网用户和 Internet 上的用户使用 SMTP 服务器发邮件。

在 USG2210 上配置 AV 功能，扫描企业内网用户和 Internet 上的用户的 SMTP 邮件中的附件，如果发现用户邮件的附件中带有病毒，则删除附件内容并在邮件正文添加宣告，避免 SMTP 邮件服务器受病毒攻击。

配置步骤

Step 1 配置 USG2210 的接口 IP 地址，并将接口加入安全区域

1) 在左侧“菜单”导航树中选择“网络”。
2) 选择“接口”页签。
3) 在“接口列表”区域框中单击接口 GE 0/0/0 对应的 。
4) 在“修改 GigabitEthernet”区域框中配置参数。



5) 单击“应用”。

6) 在“接口列表”区域框中单击以太网接口 GE 0/0/1 对应的 。

7) 在“修改 GigabitEthernet”区域框中配置参数。

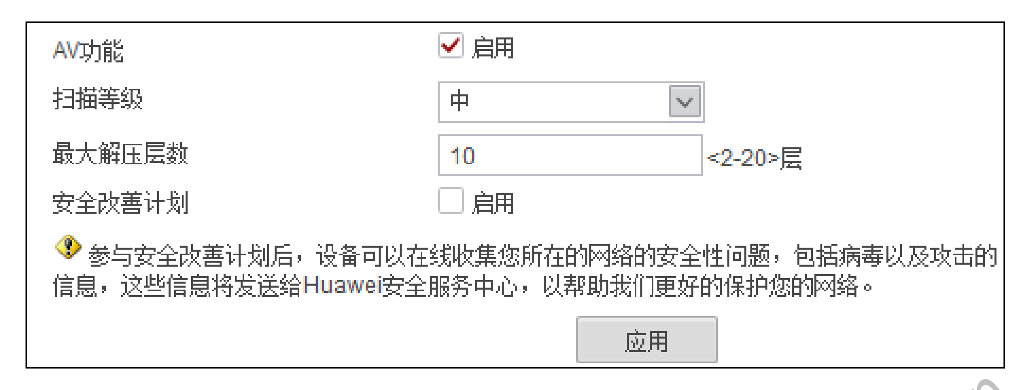


8) 单击“应用”。

Step 2 配置 AV 全局参数

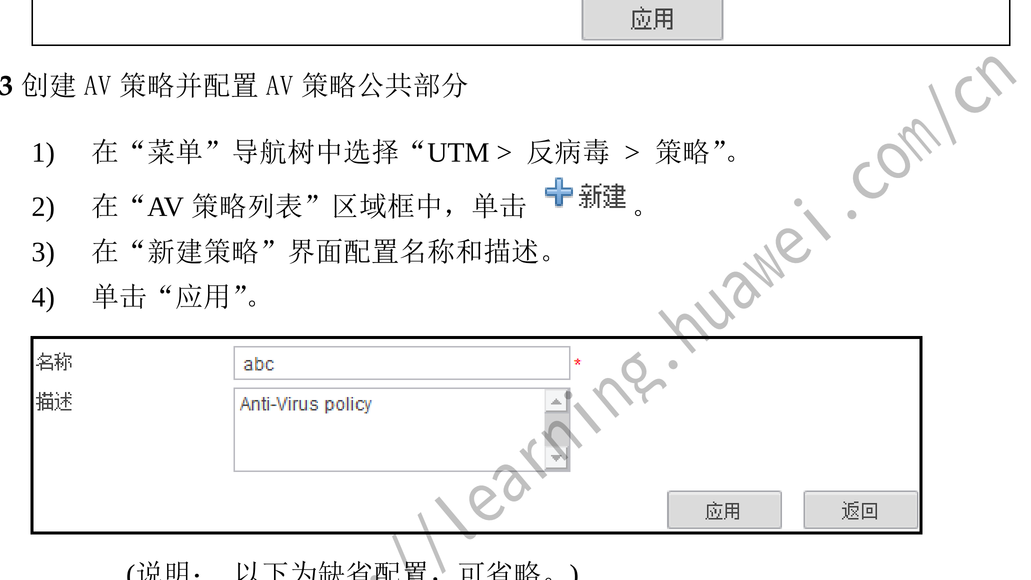
说明： 以下为缺省配置，可省略。

1) 在“菜单”导航树中选择“UTM>反病毒>策略”。
2) 在“配置全局参数”区域框中配置 AV 全局参数。



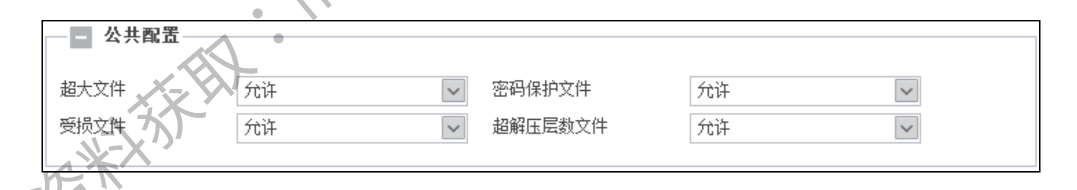
Step 3 创建 AV 策略并配置 AV 策略公共部分

1) 在“菜单”导航树中选择“UTM > 反病毒 > 策略”。
2) 在“AV 策略列表”区域框中，单击 新建 。
3) 在“新建策略”界面配置名称和描述。
4) 单击“应用”。



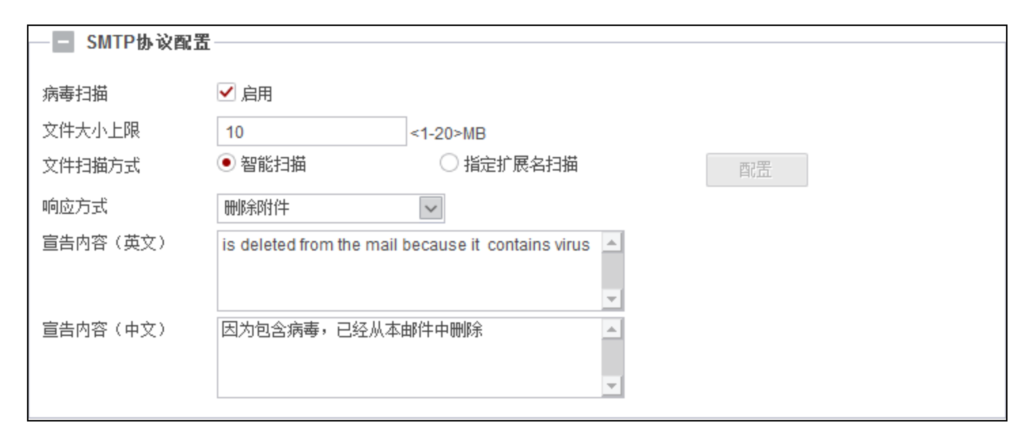
(说明： 以下为缺省配置，可省略。)

5) 在“公共配置”区域框中配置 AV 策略的公共部分。



Step 4 配置 AV 策略中各协议对应的部分

1) 在“HTTP 协议配置”区域框中去选“病毒扫描”对应的复选框，关闭 HTTP 协议的病毒扫描开关。
2) 在“FTP 协议配置”区域框中去选“病毒扫描”对应的复选框，关闭 FTP 协议的病毒扫描开关。
3) 在“SMTP 协议配置”区域框中配置各参数。



4) 在“POP3 协议配置”区域框中去选“病毒扫描”对应的复选框，关闭 POP3 协议的病毒扫描开关。

5) 单击“应用”。

Step 5 在 Trust 和 Untrust 域间应用 AV 策略，保护 SMTP 邮件服务器不受来自 Internet 上的用户的病毒攻击

1) 在“菜单”导航树中选择“防火墙 > 安全策略 > 转发策略”。

2) 在“转发策略列表”区域框中，单击 新建 。

3) 配置转发策略的参数，将 AV 策略“abc”应用在 Untrust 和 Trust 域间。





结果检查

当启用 AV 功能后，用户邮件的附件中带有病毒，则删除附件内容并在邮件正文添加宣告。

4.2 内网用户防病毒攻击实验

实验目的

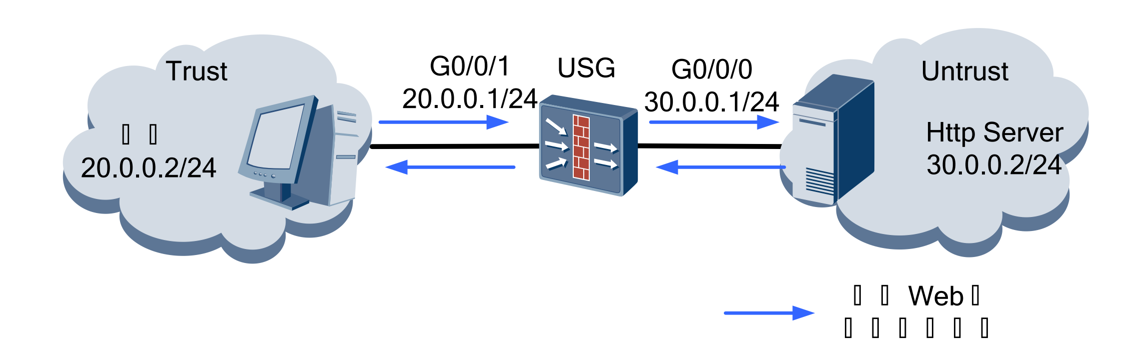
熟悉 UTM 产品的内部用户访问 Internet 上的网页时防病毒配置。

组网设备

USG2200 一台、主机两台（其中一台模拟 HTTP 服务器）

实验拓扑图

Figure 4-2 内网用户防病毒攻击实验拓扑图



- 内网位于 Trust 区域，HTTP 服务器位于 Untrust 区域。
- 在 USG2200 上配置 AV 功能，当内网用户访问的网页带病毒时，USG2200 中断访问，并向用户推送一个警告页面提示访问的网页中含病毒。

配置步骤

Step 1 配置 USG2200 的接口 IP 地址，并将接口加入安全区域，配置略，请参见 4.1.4

Step 2 配置缺省路由。配置略，请参见 4.1.4

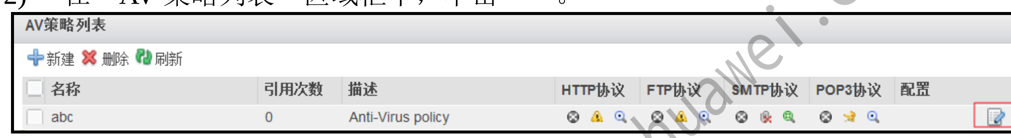
Step 3 配置 AV 全局参数

配置略，请参见 4.1.4

Step 4 创建 AV 策略并配置 AV 策略公共部分

1) 在“菜单”导航树中选择“UTM > 反病毒 > 策略”。

2) 在“AV 策略列表”区域框中，单击 。



Step 5 配置 AV 策略中各协议对应的部分

1) 在“SMTP 协议配置”区域框中 取消复选框。



2) 在“HTTP 协议配置”区域框中配置各参数。



3) 单击“应用”。

Step 6 在 Trust 和 Untrust 域间应用 AV 策略，保护内网主机不受病毒侵害

1) 在“菜单”导航树中选择“防火墙 > 安全策略 > 转发策略”。

2) 在“转发策略列表”区域框中，单击 新建 。

3) 配置转发策略的参数，将 AV 策略“abc”应用在 Trust 和 Untrust 域间。

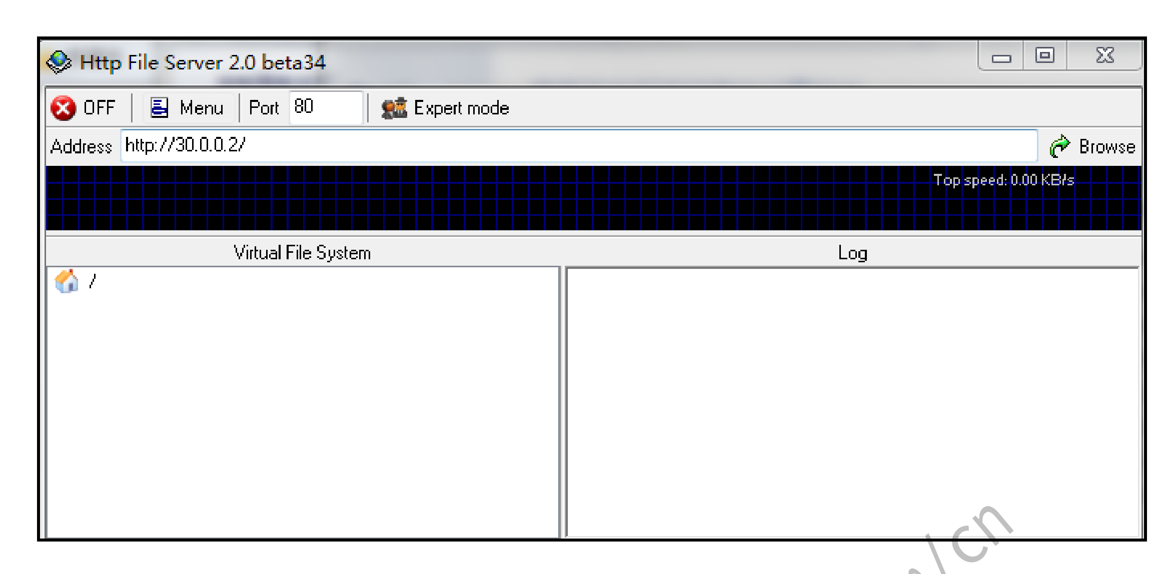
4) 单击“应用”。



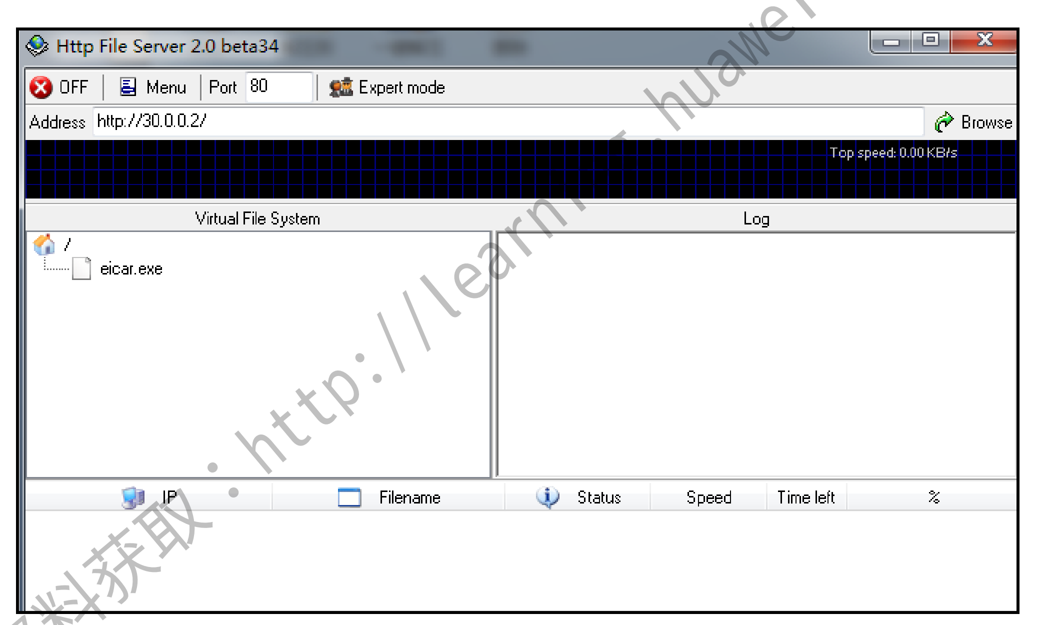
Step 7 在 Web 服务器端搭建 Http 服务器，并且放置病毒测试文件。

注：Http 服务器可以用 Hfs(Http file Server)代替，病毒测试文件可以通过 www.eicar.org 网站下载。

1) 在服务器端，安装 Hfs 软件，选择指定的 IP 地址和端口号。



2) 将病毒测试文件直接拖入 hfs 窗口中，完成 hfs 加载病毒测试文件 eicar.exe。并点击开关，将 Off 变成 ON 状态。



3) 客户端 PC 通过 http://30.0.0.2/eicar.exe 测试，提示是发现病毒。

Scan for Network Security

Warning: 该网页包含病毒，已被禁止访问，如有异议，请联系IT管理员，电话8888..
Reason: The virus (EICAR Test String) is detected in the file(eicar.exe).

结果检查

启用 AV 功能后，当用户访问的网页带病毒时，USG2200 中断访问，并向用户推送一个警告页面提示访问的网页中含病毒

5 URL 过滤实验

5.1 配置 URL 过滤实验

实验目的

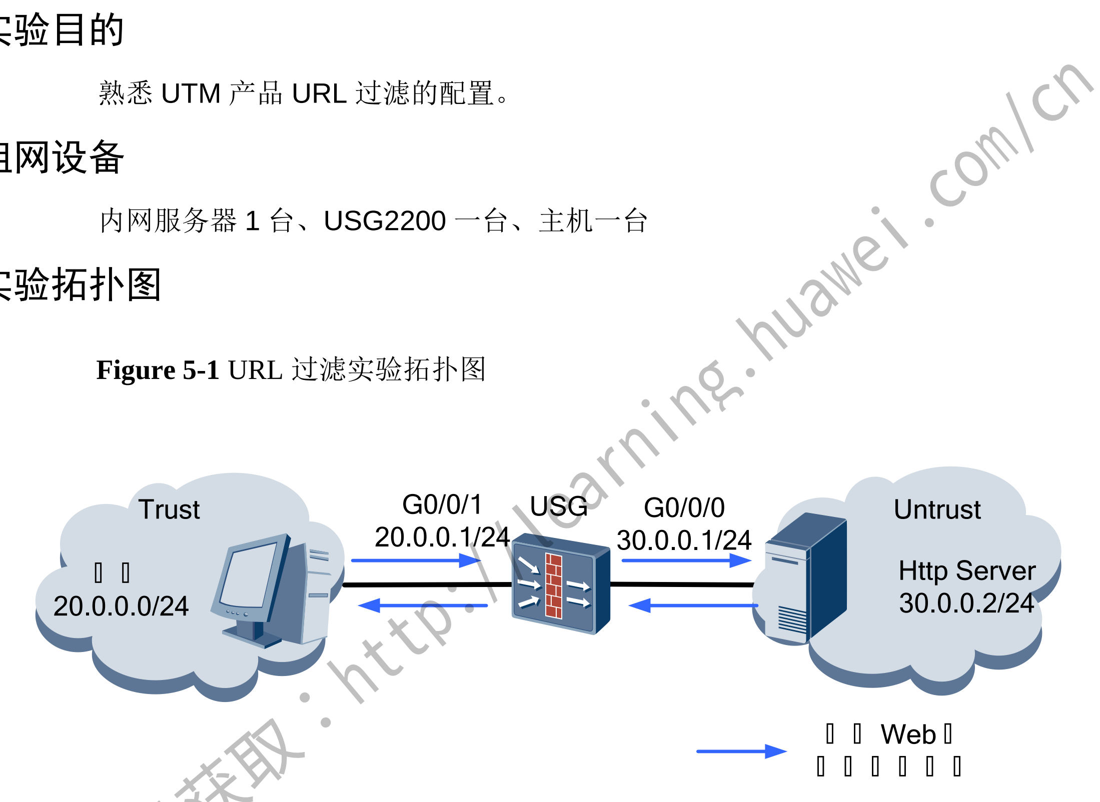
熟悉 UTM 产品 URL 过滤的配置。

组网设备

内网服务器 1 台、USG2200 一台、主机一台

实验拓扑图

Figure 5-1 URL 过滤实验拓扑图



公司有研发用户和非研发用户两类，研发用户对应的 IP 地址范围是 20.0.0.10/24～20.0.0.100/24，非研发用户对应的 IP 地址范围是 20.0.0.101/24～20.0.0.200/24。

具体需求如下：

- 企业所有员工可以访问 www.information.com 网站。
- 企业所有员工不可以访问 www.bt.com 网站。
- 研发用户在每天的 8：00～18：00 不可以访问社会焦点类网站和 www.abcd.com，在 12：00～20：00 不可以访问 P2P 类网站。
- 非研发用户在每天 8：00～18：00 不可以访问体育类网站。

配置步骤

Step 1 配置 URL 过滤基本参数

1) 在“菜单”导航树中选择“UTM > WEB 过滤 > 策略”。
2) 在“web 过滤基本配置”区域框中配置 URL 过滤基本参数。



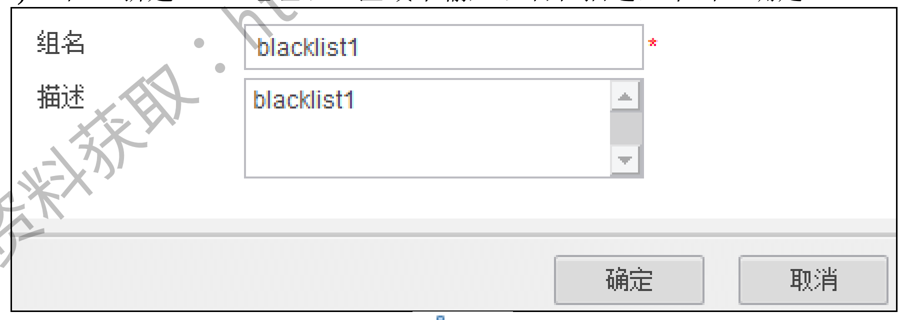
3) 单击“应用”。

Step 2 配置黑白名单。

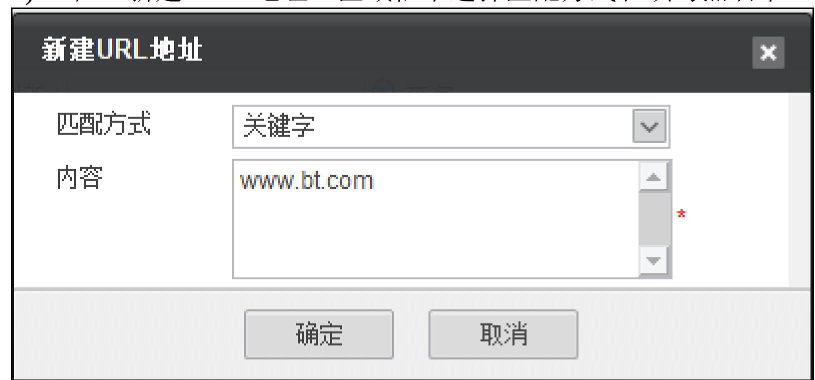
1) 在“菜单”导航树中选择“UTM > WEB 过滤 > URL 过滤器”。
2) 在“新建 URL 过滤器”区域中输入名称和描述。
3) 点击“应用”。



4) 单击“URL 黑名单”后面对应的 。
5) 在“黑名单配置”区域点击 新建 。
6) 在“新建 URL 地址组”区域中输入组名和描述，单击“确定”。



7) 在 URL 地址列表区域，单击 新建 。
8) 在“新建 URL 地址”区域框中选择匹配方式和填写黑名单 URL。

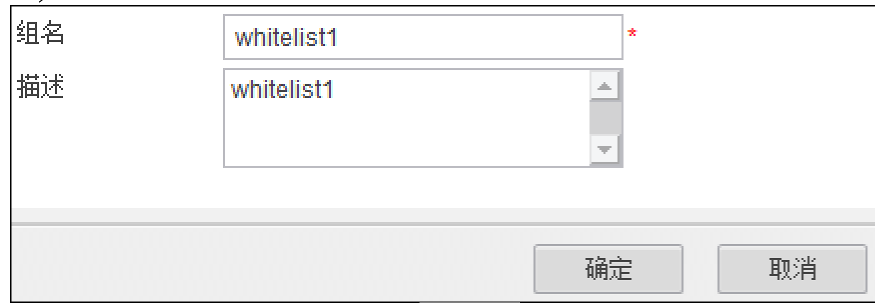


9) 单击“确定”。 一直回到“修改过滤器”界面。

10) 单击“URL 白名单”后面对应的 。

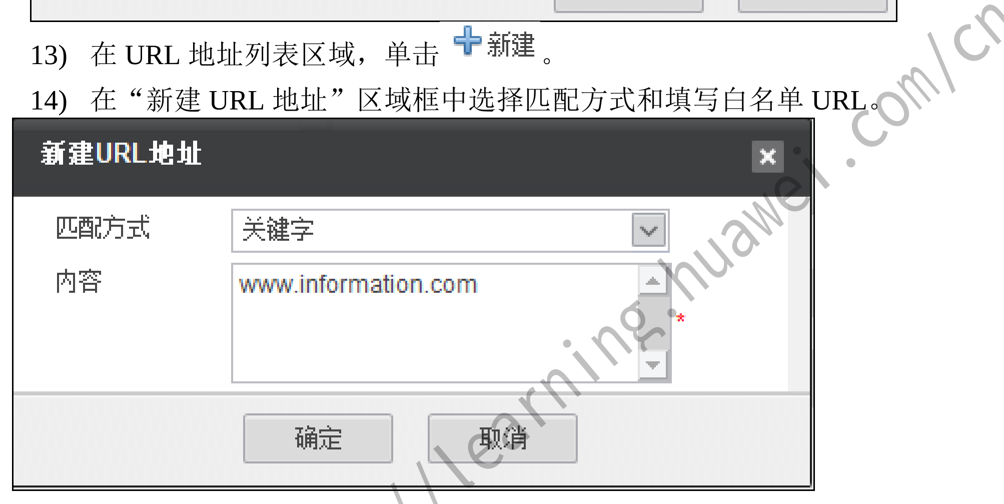
11) 在“白名单配置”区域点击 新建 。

12) 在“新建 URL 地址组”区域中输入组名和描述，单击“确定”。



13) 在 URL 地址列表区域，单击 新建 。

14) 在“新建 URL 地址”区域框中选择匹配方式和填写白名单 URL。



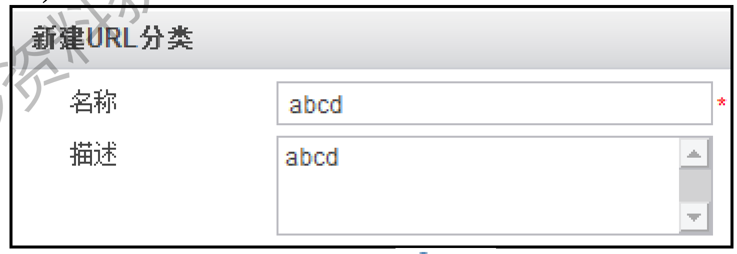
15) 单击“确定”。 一直回到“修改过滤器”界面。

Step 3 配置 URL 分类。

1) 在“菜单”导航树中选择“UTM > WEB 过滤 > URL 分类”。

2) 在“URL 分类列表”区域中点击 新建 。

3) 在“新建 URL 分类”中输入名称和描述。



4) 在“已选”区域下方点击 新建 。

5) 在“新建 URL 地址组”区域中输入组名和描述，单击“确定”。

6) 在 URL 地址列表区域，单击 新建 。

7) 在“新建 URL 地址”中输入关键字和内容。

新建URL地址

匹配方式　关键字

内容　www.abcd.com *

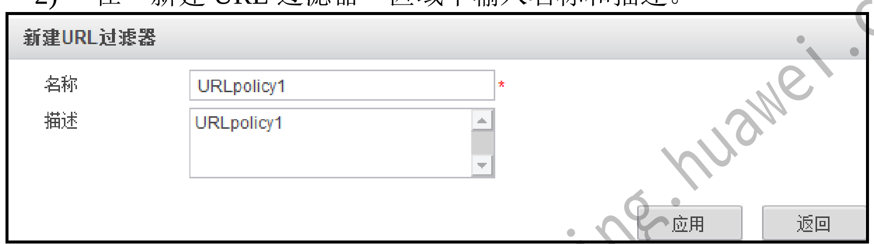
确定　取消

8)　单击“确定”，一直回到“URL 分类列表”界面。

Step 4 配置 URL 过滤器。

1)　在“菜单”导航树中选择“UTM > WEB 过滤 > URL 过滤器”。

2)　在“新建 URL 过滤器”区域中输入名称和描述。



3)　点击“应用”。

4)　在“修改 URL 过滤器”区域，配置参数。



控制选项	控制内容	修改
URL白名单	whitelist1	
URL黑名单	blacklist1	

5)　在“分类名称”区域，点击分类名称后面对应的 ，切换处理动作。



分类名称	描述	处理动作	配置
abcd	abcd	阻断	
P2P	Web sites related to P2P	允许	
下载	Web sites related to kinds of download	允许	
人文	Web sites related to kinds of culture(arts,history,etc.)	允许	
体育/运动	Web sites related to kinds of Sports	允许	
社会焦点	Web sites related to kinds of Social Focus(social issue,ecology,human righ...	阻断	
军事	Web sites related to military	允许	
社交网络	Web sites related to SNS	允许	
博彩	Web sites related to lottery	允许	
休闲	Web sites related to recreation(games,cartoon,chat,dating, etc.)	允许	
宗教	Web sites related to religion	允许	
性题材	Web sites related to sex but not porn	允许	

6)　点击“应用”。

7)　重复 2-6 项，创建 URL 过滤器 urlpolicy2，配置 P2P 分类访问控制动作都为阻断；创建 URL 过滤器 urlpolicy3，配置体育/运动分类访问控制动作为阻断；创建 URL 过滤策略 urlpolicy4，所有分类控制动作均为允许。

Step 5 配置 DNS 服务器。

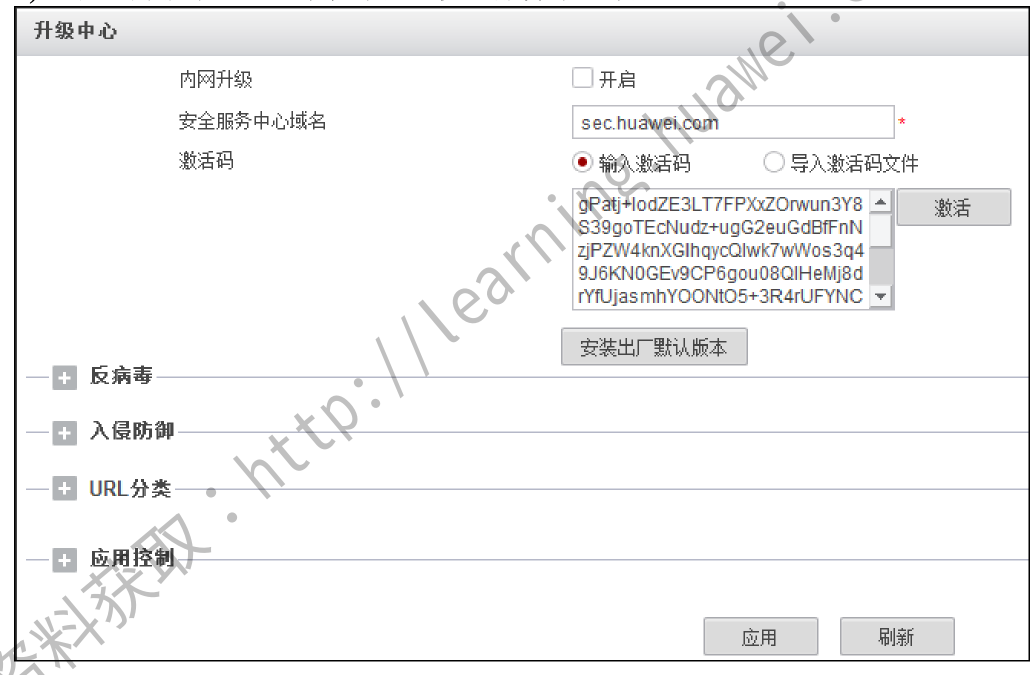
1) 在“菜单”导航树中选择“网络 > DNS”。
2) 在“服务器列表”区域中输入 DNS 地址，点击“添加”。



说明： DNS 服务器 IP 地址 202.118.66.6 只是该举例中的地址，实际配置中根据用户具体 DNS 服务器地址配置。

Step 6 配置安全服务中心。

1) 在“菜单”导航树中选择“系统 > 维护”。
2) 选择“升级中心”页签。
3) 在“升级中心”区域框中配置安全服务中心域名。



4) 单击“应用”。

Step 7 配置时间段

1) 在“菜单”导航树中选择“防火墙 > 时间段”。
2) 在“时间段”区域框中单击 新建 。
3) 在“时间段”区域框中配置时间段 time1。

新建时间段

名称 time1 *

应用 返回

4) 单击“应用”。
5) 在“时间段列表”区域，点击 新建 。
6) 在“时间段”区域窗口完成参数配置。



7) 单击“确定”。

8) 重复 2)~7)，配置时间段 time2。

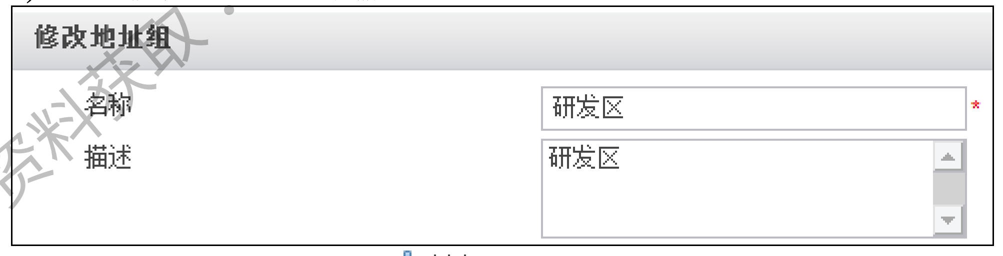
Step 8 配置地址对象

1) 在“菜单”导航树中选择“防火墙 > 地址”。

2) 选择“地址组”页签。

3) 单击“地址组列表”区域框中的 新建 。

4) 在“修改地址组”区域输入名称、描述。



5) 在“配置地址”区域点击 新建，输入研发区地址段。



6) 单击“应用”。

7) 重复 3)~5)，配置地址对象“非研发区”。

Step 9 在 Trust 与 Untrust 域间应用 URL 过滤策略

1) 在“菜单”导航树中选择“防火墙 > 转发策略”。

2) 单击“转发策略”区域框中的 新建 。

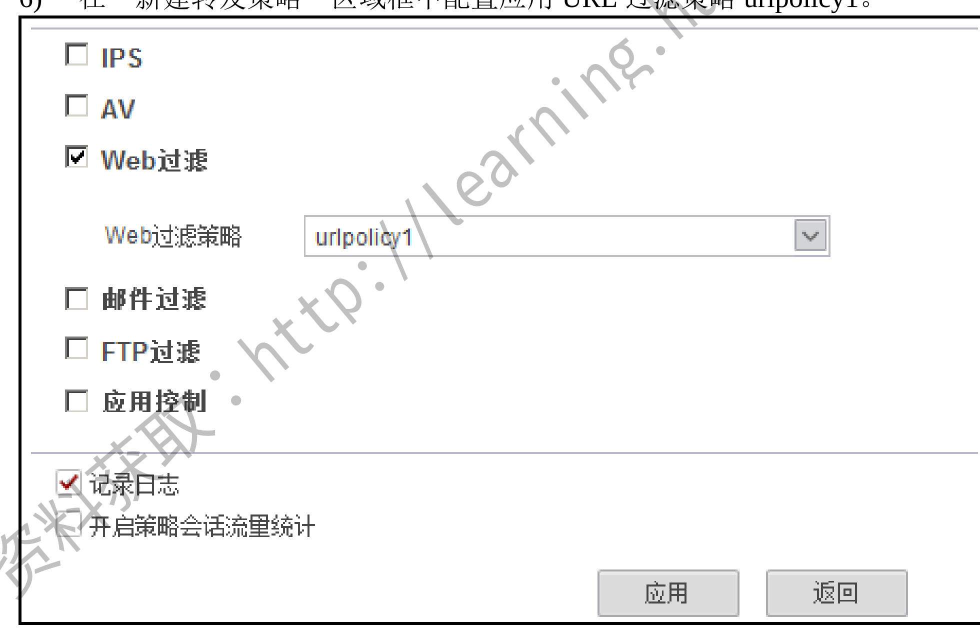
3) 在“新建转发策略”区域，选择源地址和目的地址为“研发区”地址组。

4) 在“新建转发策略”区域，选择时间为“time1”。

5) 在“新建转发策略”区域，选择动作为“permit”。

源安全区域	trust *	
目的安全区域	untrust *	
源地址	研发区	多选
目的地址	any	多选
用户	请选择或输入用户或用户组	多选
服务	请选择服务	多选
时间段	time1	
动作	permit *	
描述		

6) 在“新建转发策略”区域框中配置应用 URL 过滤策略 urlpolicy1。



7) 选中“记录日志”前面的复选框。

8) 单击“应用”。

9) 重复 2)～8)，配置应用 URL 过滤策略 urlpolicy2、urlpolicy3、urlpolicy4。

结果检查

通过配置黑白名单、自定义分类和预定义分类的访问控制动作，对员工的 HTTP 请求进行 URL 过滤，可以实现对企业员工上网行为的管理。

6 RBL 过滤配置实验

6.1 配置预定义方式 RBL 过滤

实验目的

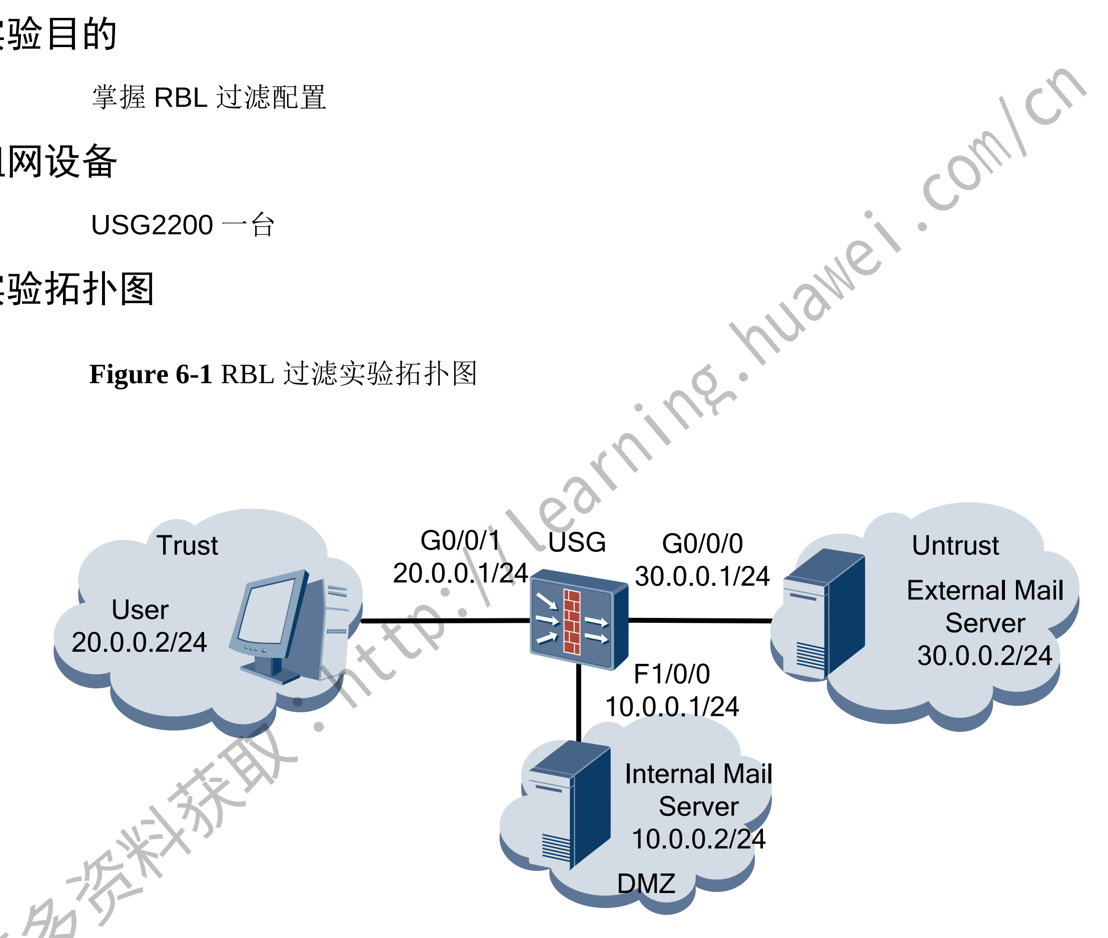
掌握 RBL 过滤配置

组网设备

USG2200 一台

实验拓扑图

Figure 6-1 RBL 过滤实验拓扑图



如图 6-1 所示，USG 部署在企业网出口处。要求 USG 对进入企业内部的邮件进行过滤，以保护内部邮件服务器和内网用户。具体需求如下：

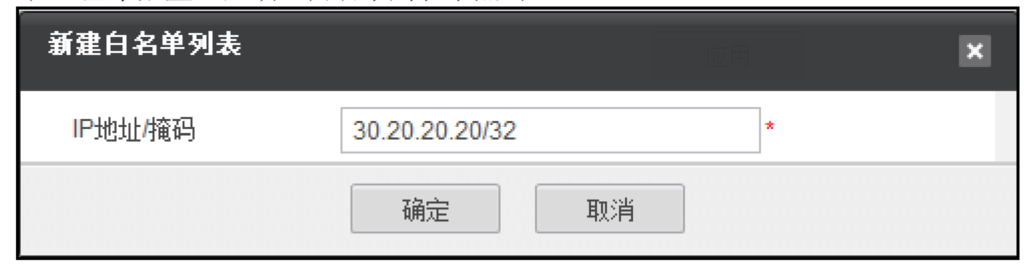
- USG 通过预定义的 RBL 服务器实现邮件过滤，保护邮件服务器和内网用户不受垃圾邮件的侵扰。
- 在任何情况下，允许源地址为 30.20.20.20 的用户发送邮件给内网用户。
- 当邮件命中 RBL 服务器的黑名单时，阻断该邮件。

配置步骤

Step 1 配置 USG 的接口信息（略）

Step 2 配置 RBL 地址白名单

1) 在“菜单”导航树中选择“UTM > 垃圾邮件 > 垃圾邮件过滤”。
2) 在“基本配置”区域，白名单列表中点击 新建 。



3) 点击“确定”。

Step 3 启用 RBL 过滤，配置查询 RBL 的 DNS 服务器的 IP 地址

1) 在“菜单”导航树中选择“UTM > 邮件过滤 > 垃圾邮件过滤”,选择“基本配置”页签。
2) 在“基本配置”区域框中，启用垃圾邮件过滤功能、白名单、黑名单，配置 DNS 服务器。具体配置如图所示。



注：查询垃圾邮件服务器的 DNS 地址，根据实际的 DNS 去配置。DNS 地址一般由运营商提供。

3) 单击“应用”。

Step 4 配置预定义策略

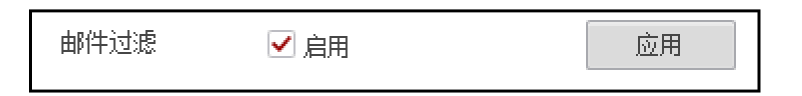
1) 在“菜单”导航树中选择“UTM > 邮件过滤 > 垃圾邮件过滤”,选择“过滤策略”页签。
2) 在“预定义策略列表”区域框中，点击“预定义策略”对应的 。启用预定义策略，并配置策略的动作为“阻断”。具体配置如图所示。



3) 单击“应用”。

Step 5 配置邮件过滤策略

1) 在“菜单”导航树中选择“UTM＞ 邮件过滤 ＞ 策略”,在“基本配置”区域，选择启用邮件过滤，点击“应用”



2) 在“邮件过滤策略列表”区域，选择 新建，输入名称和描述，点击“应用”

名称 RBList1 *
描述 RBList1
应用 返回

3) 在“修改邮件过滤策略”区域，选择“垃圾邮件过滤”，发送和接收匿名邮件为阻断。

垃圾邮件过滤（此功能需要License）
发送匿名邮件 阻断
接收匿名邮件 阻断

4) 根据需要配置邮件过滤选项，最后点击应用。



Step 6 在域间应用预定义策略

1) 在“菜单”导航树中选择“防火墙 > 安全策略”，选择“转发策略”页签。

2) 单击 新建，在 Untrust 到 DMZ 区域方向应用预定义策略。具体配置如图所示。

防火墙 > 安全策略 > 转发策略

新建转发策略

源安全区域	untrust *	
目的安全区域	dmz *	
源地址	请选择或输入IP地址	多选
目的地址	10.0.0.2/32	多选
用户	请选择或输入用户或用户组	多选
服务	请选择服务	多选
时间段	all	
动作	permit *	
描述		

- ☐ IPS
- ☐ AV
- ☐ Web过滤
- ☑ 邮件过滤
  - 邮件过滤策略 rbllist1
- ☐ FTP过滤
- ☐ 应用控制

- ☐ 记录日志
- ☐ 开启策略会话流量统计

应用 返回

3) 单击“应用”。

Step 7 配置 DMZ 和 Trust 的 Outbound 方向的防火墙策略，允许内网用户从邮件服务器下载邮件

1) 在“菜单”导航树中选择“防火墙 > 安全策略”，选择“转发策略”页签。

2) 单击 新建，在 Trust 到 DMZ 区域方向配置防火墙策略。具体配置如图所示。

防火墙 > 安全策略 > 转发策略

新建转发策略

源安全区域	trust *	
目的安全区域	dmz *	
源地址	请选择或输入IP地址	多选
目的地址	10.0.0.2/32	多选
用户	请选择或输入用户或用户组	多选
服务	请选择服务	多选
时间段	all	
动作	permit *	
描述		

☐ IPS

☐ AV

☐ Web过滤

☑ 邮件过滤

邮件过滤策略 rbllist1

☐ FTP过滤

☐ 应用控制

☐ 记录日志

☐ 开启策略会话流量统计

应用 返回

3) 单击“应用”。

结果检查

- 源地址为 30.20.20.20 的用户可以发邮件给内网用户。
- 当发送给内网用户和内部邮件服务器的邮件命中 RBL 服务器的黑名单时，该邮件被阻断。

7 DPI 配置实验

7.1 配置 DPI 升级

实验目的

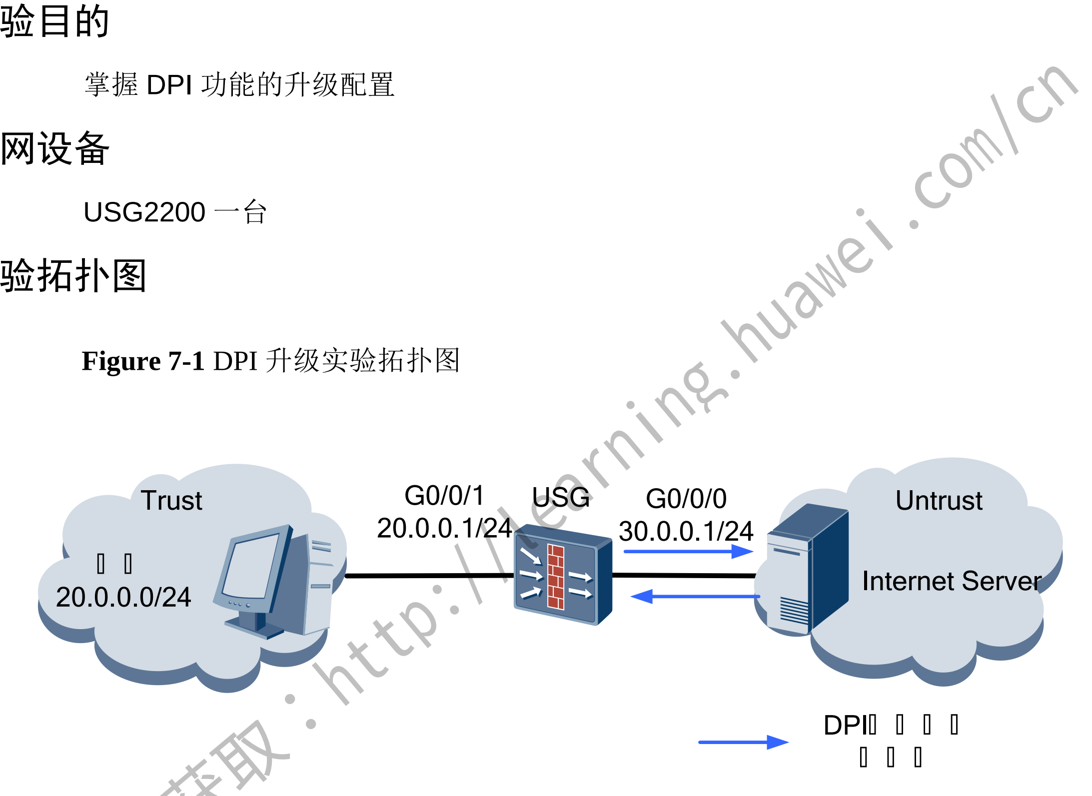
掌握 DPI 功能的升级配置

组网设备

USG2200 一台

实验拓扑图

Figure 7-1 DPI 升级实验拓扑图



配置步骤（命令行）

Step 1 执行命令 system-view，进入系统视图

Step 2 执行命令 dns resolve，启用动态 DNS 解析功能

Step 3 执行命令 dns server ip-address，指定 DNS 服务器

Step 4 执行命令 dpi，进入 DPI 视图

Step 5 可选：执行命令 using default rule-base update server，将 DPI 升级服务器设为默认升级服务器。 默认升级服务器为 sec.huaweisymantec.com

Step 6 执行命令 update rule-base server { domain domain-name [port port-number] | ip-address ip-address [port port-number] }*，配置升级服务器的域名或者 IP 地址，最多可配置 3 个，在升级时将依次尝试

Step 7 可选：执行命令 update rule-base remote，立即远程升级 DPI 知识库

Step 8 执行命令 update rule-base remote period period-val，配置自动升级的更新周期

Step 9 可选：执行命令 update rule-base no-save，配置此命令后，设备将不保存升级后的 DPI 知识库 。

配置步骤（Web）

Step 1 依次点击系统-维护-升级中心。（略）配置步骤详见 3.1。



结果检查

执行命令 **display dpi verbose**，查看 DPI 模块的配置情况：

```
[USG-dpi] display dpi verbose

DPI verbose information:

------------------------------------------------------

  DPI Engine Version                  : DPI-Module V100R001C02SPC008

  DPI Current Detect Max PktNum       : 20

  DPI Session Current Flow Number : 7

  DPI Update Period                   : 90

  Save Rule-base After Updated        : no

  DPI Update Server                   :
```

```
      Server 1 : 1.1.1.1 80

      Server 2 : 2.2.2.2 80

      Server 3 : 3.3.3.3 80

------------------------------------------------------
```

设备完成升级后，执行命令 **display dpi brief**，查看 DPI 知识库的当前版本信息和升级日期情况。

```
[USG] display dpi brief

DPI brief information:

------------------------------------------------------

   DPI enabled                            : yes

   Rule-Base's Current Version : 1.0.0.108

   Rule-Base's load time              : 2010/05/31 11:43:58

   Rule-Base's publish time         : 2010/01/30 10:42:54

------------------------------------------------------
```

7.2 配置 DPI 控制 IM 行为

实验目的

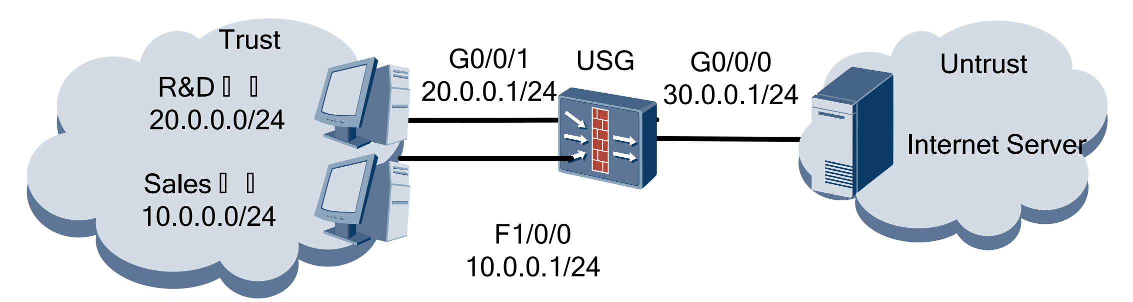
掌握 DPI 功能应用配置

组网设备

USG2200 一台

实验拓扑图

Figure 7-2 DPI 控制 P2P 行为和流媒体实验拓扑图



内网研发部门人员在工作时间周一至周五的 8:00～12：30，14：00-18:00 不能使用 IM（Instant Messaging）功能。

内网销售部门人员在所有工作时间可以正常使用 IM 功能。

配置步骤

Step 1 配置 USG 使内网用户可以访问因特网，具体步骤略。

Step 2 配置时间范围，设定为周一至周五的 8:00-12：30，14：00-18:00，命名为 work_time。

1) 选择“防火墙 > 时间段 > 时间段”。
2) 在“时间段列表”中单击 。
3) 在“名称”中输入时间段的名称 work_time。
4) 单击“应用”。
5) 单击 ，创建时间段 work_time 的上午部分，如图 1 所示。
6) 单击“确定”。

图 1 新建时间段一



7) 再单击 ，创建时间段 work_time 的下午部分，如图 2 所示。
8) 单击“确定”。

图 2 新建时间段一

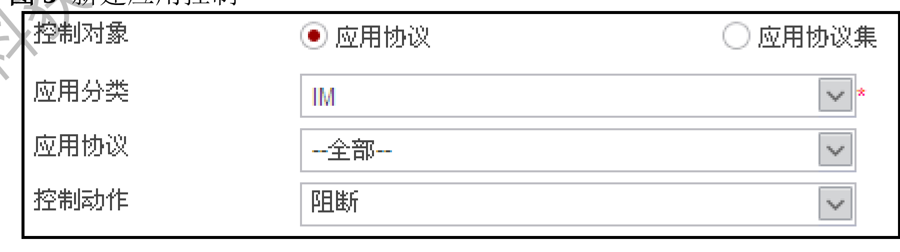


Step 3 启用应用控制功能，并配置应用控制策略 im_block，对 IM 类型的协议进行检测，并对检测到的 IM 协议执行阻断动作。

1) 选择“UTM > 应用控制 > 策略”。
2) 选择“应用控制功能”后的“启用”复选框。
3) 单击“应用”。
4) 在应用控制策略列表中，单击 ，创建应用控制策略 im_block。
5) 单击“应用”。
6) 在应用控制列表中，单击 ，创建应用控制，如图 3 所示。
7) 单击“确定”。
8) 单击“应用”。



图 3 新建应用控制



Step 4 配置转发策略，在域间应用 DPI 策略 im_block，实现对 20.0.0.0/24 网段的研发人员在 work_time 时间段内的 IM 即时通讯的阻断。

1) 选择“防火墙 > 安全策略 > 转发策略”。
2) 选择“转发策略”页签。
3) 在“转发策略列表”中，单击 ，参数配置如图 4 所示。
4) 单击“应用”。

图 4 新建转发策略

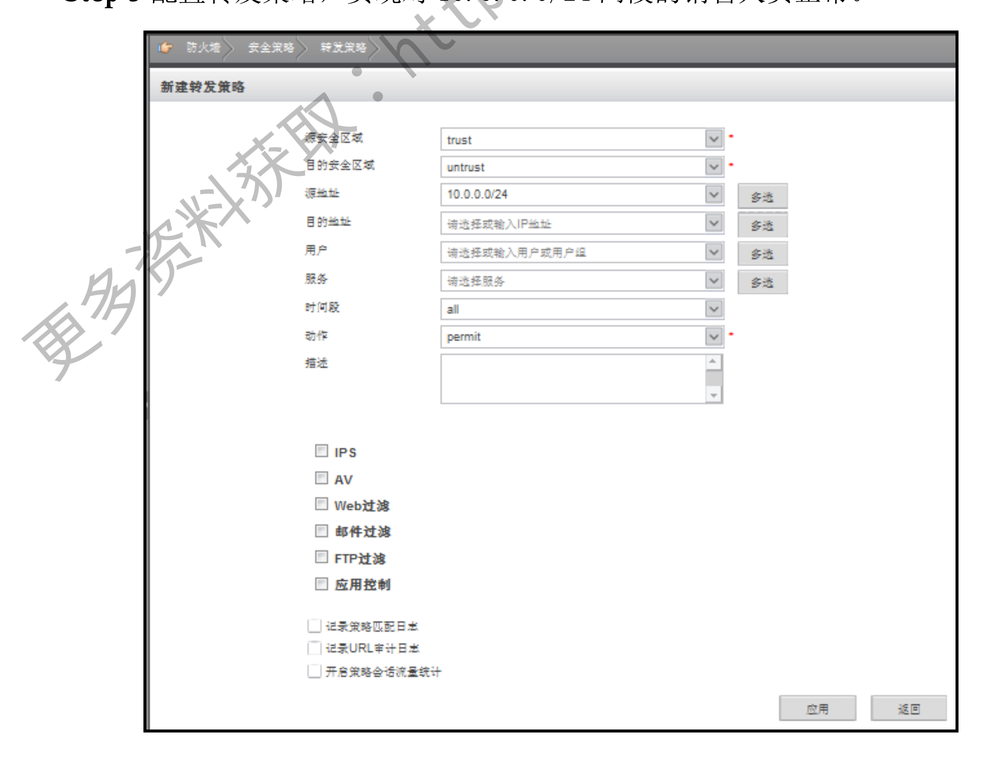
源安全区域 trust *
目的安全区域 untrust *
源地址 20.0.0.0/24 多选
目的地址 请选择或输入IP地址 多选
用户 请选择或输入用户或用户组 多选
服务 请选择服务 多选
时间段 all
动作 permit *
描述

IPS
AV
Web过滤
邮件过滤
FTP过滤
应用控制

应用控制策略 im_block

记录日志
开启策略会话流量统计

Step 5 配置转发策略，实现对 10.0.0.0/24 网段的销售人员正常。

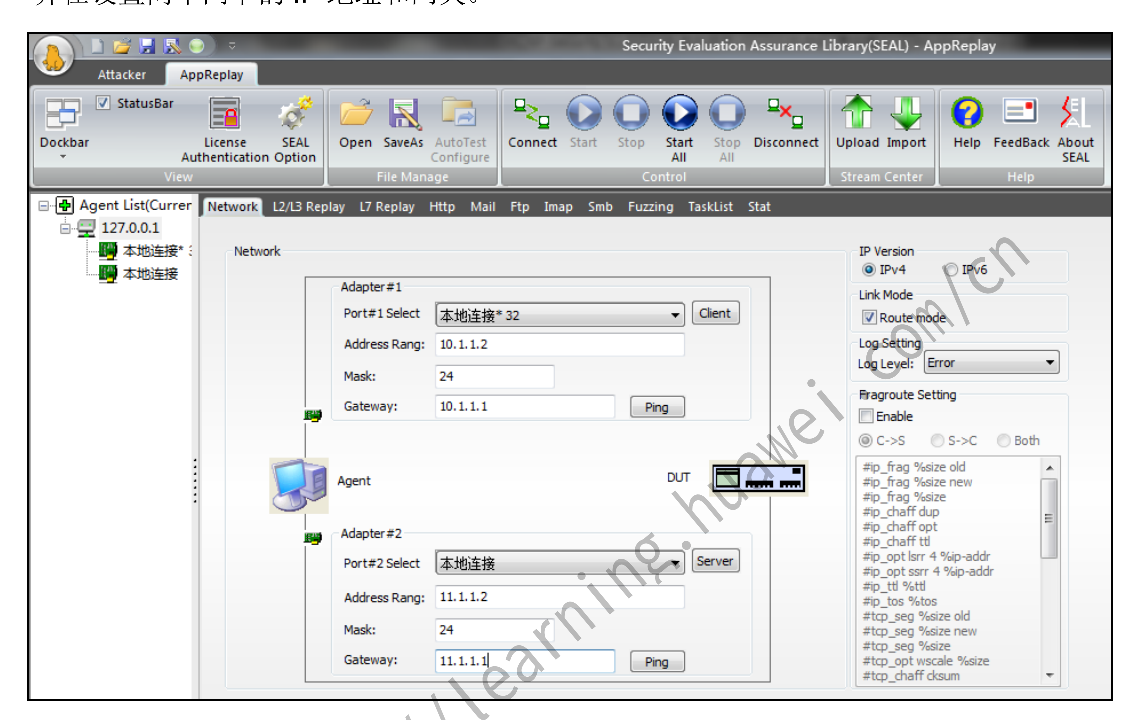


Step 6 在 Untrust 区域放置一台 PC 机器，启动 Sear 的 AppReplay 组件模拟 P2P 和流媒体服务器。

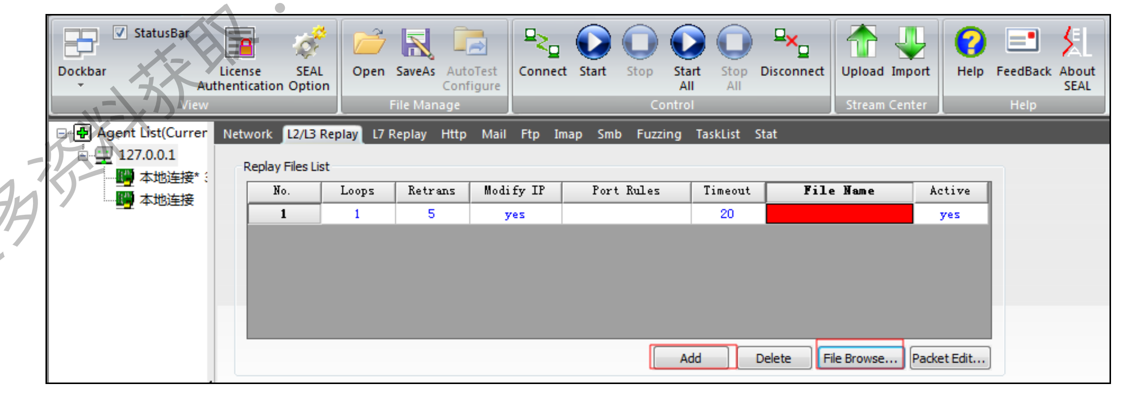
1) 启动 Sear 的 AppReplay 组件。

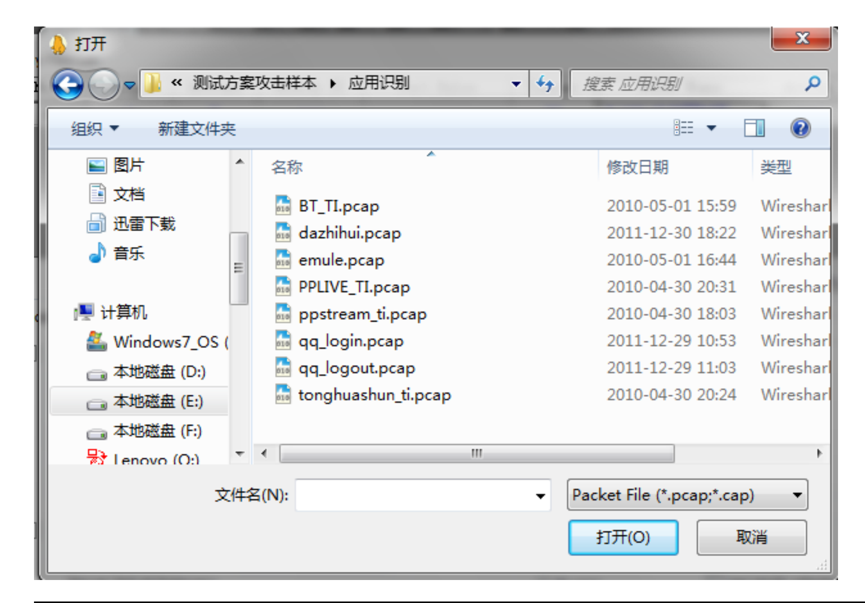
Link Mode 选择 Route Mode，Route Mode 需要设置网关。

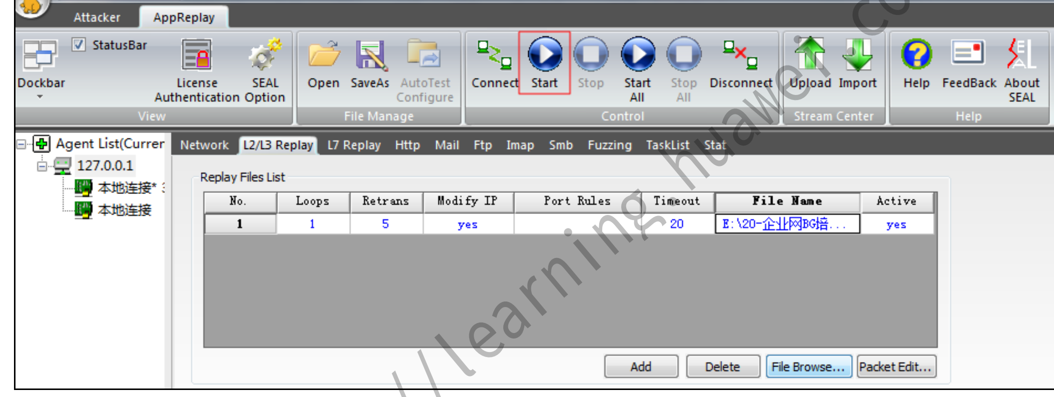
并在设置两个网卡的 IP 地址和网关。



2) 选择 L2/L3replay 点击 Add 按钮，点击 File Browser，添加攻击模拟包。并点击开始  按钮。







结果检查

配置完成后，在工作时间和非工作时间在 192.168.2.0/24 网段的主机上使用 QQ、MSN 等即时通讯工具，如均可正常使用，则表示设备的配置对销售部门的 IM 使用无影响。

在工作时间在 192.168.1.0/24 网段主机上使用即时通讯工具，如无法使用，则表示设备在工作时段对研发部门的 IM 使用成功阻断。

在非工作时间在 192.168.1.0/24 网段主机上使用即时通讯工具，如可正常使用，则表示设备在非工作时段对研发部门的 IM 使用不进行阻断。

8 UTM 特性故障排除实验

8.1 UTM 特性故障排除

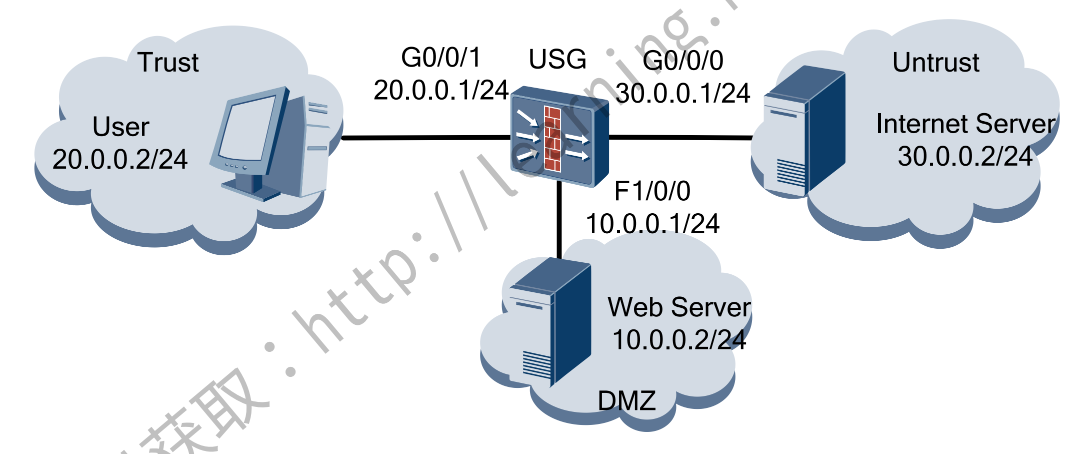
实验目的

掌握防火墙 UTM 特性常见故障排除

组网设备

1 台 UTM(USG2200)，一台 USG2130（模拟 internet 出口）；2 台 PC（模拟内网用户和 web 服务器）。

实验拓扑图



UTM 工作在路由模式，用户网段为 20.0.0.0/24,位于 trust 区域。WEB 服务器网段为 10.0.0.0/24，位于 DMZ 区域。外网位于 Untrust 区域，内网用户和服务器的网关都在出口 USG2230 上。为了保护内网用户和服务器不受病毒入侵，在 trust 和 untrust 以及 untrust 和 DMZ 域间开启了 AV 功能。为了限制内网用户访问 internet 地址，在 trust 和 untrust 域间开启了 url 过滤功能（URL 地址通过将 USG2230 的 web 登陆界面来模拟, http://30.0.0.2/。

故障排除流程

Step 1 故障现象描述

- Trust 区域用户无法访问 DSM 区域的 WEB 服务器 http://10.0.0.2；
- Trust 区域 URL 过滤不生效，仍然可以访问 http://30.0.0.2。

Step 2 故障相关信息收集及分析

根据基本故障现象的描述，利用各种方法进一步收集相关信息，定位故障。

1) 故障点：

2） 信息收集方法及命令：

3） 信息中的关键证据：

Step 3 故障排除流程

请根据已知的故障现象和经验进行原因分析，并列举每一故障现象的可能原因：

1） 故障现象：

2） 原因列表：

3） 排除过程：

讲师实验指导建议

Step 1 分组建议

由于本实验共需 2 台 USG，建议 2－3 人一组。

Step 2 组长推举以及组员分工

在分组之后，需要推举出一个组长来领导各组完成实验。组长在本组的实验过程中主要起一个牵头的作用，并组织组内的讨论。组长的推举可以采取学员毛遂自荐的方式，如果学员反应不积极，也可以有意识的指定学员中技术水平较好的来担任组长，以保证实验的顺利进行。在推举出组长之后，还可以引导组长对自己的组员也进行相应的分工。比如说可以让特定的组员负责查看配置与 display 信息；某些组员负责实际操作，修改配置；某些组员负责记录故障点和每一步操作，完成实验报告。

Step 3 分组讨论

在实验的开始阶段，讲师应该要求各组的组长带领各组的组员先弄清网络的状况与要求，并把各设备上的配置都先读一遍，这样才不会在后面的实验中大家都弄得一头雾水。接下来可以让组长组织对故障现象，故障定位和如何解决问题进行组内的讨论。同时讲师也应该时刻关注各组的讨论情况和实验进展，并在必要的时候参与进来，把大家引导到正确的思路上

来。因此，在分组讨论排除故障阶段，根据具体情况，可能会需要一到两名讲师指导实验以保证实验效果。

Step 4 各组总结

在实验完成之后，可以请各组的组长分别对本组的实验情况作一个经验总结，包括故障的定位过程以及如何排除故障。讲师在这个时候可以鼓励各组的组员积极的对组长的发言进行补充，讲师自己也可以针对学员的总结进行一些点评和补充。

Step 5 提问

在各组完成总结之后，讲师可以有针对性的提一些问题，以加深学员的理解，下面列出一些问题，以供参考：

参考问题：

1．GRE OVER IPSEC 和 L2TP OVER IPSEC 的 Security ACL 要如何配置，为什么要这么配置？

2．为什么要添加通过 tunnel 口的路由，缺省路由为什么不行？

Step 6 讲师总结

在本实验的最后，讲师还应该对整个实验的故障排除思路，故障点分析和解决方案做一个最终的总结，以加深学员对课程的理解，并使之更系统化。

Step 7 实验中的时间点控制

本章节实验时间建议：

- 2 小时：讲师准备好实验环境，设置好故障点。
- 10 分钟：讲师介绍实验的网络状况和具体要求，向学员描述故障现象以及实验要求。分组并选举组长，明确各组员工的分工。
- 2 小时：各组长组织组员验证故障现象，熟悉网络状况和具体配置。对故障现象，故障定位和如何解决问题进行组内讨论，最终排除故障并完成实验报告。

30 分钟：各小组选举代表对故障排除结果及过程进行分享发表，讲师进行总结和点评。

华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*）享有如下特权：

- **1、华为E-learning 课程学习**
  - **内容：所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式：***关联证书*后，请提交您的“华为账号”和注册账号的“email”到 *Learning@huawei.com 申请权限。*
- **2、华为培训教材下载**
  - **内容：华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式：**登录*华为在线学习网站*，进入“*华为培训/面授培训*”，在具体课程页面即可下载教材。
- **3、华为在线公开课(LVC)优先参与**
  - **内容：**企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式：**开班计划及参与方式请详见*LVC排期*
- **4、学习工具 eNSP**
  - eNSP (Enterprise Network Simulation Platform)，是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外，华为建立了知识分享平台 华为认证论坛。您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。（http://support.huawei.com/ecommunity/bbs/list_2247.html）

